PUBLIC RECORD OFFICE

Group/Class ..... HW 40

Piece 181

Papers relating to the post-war period retained under S3(4) of the PRA (1958)

(date) 11/2/2004

(Signed) .....

15(a)

20 Grosvenor Square.

(23)

A8/mdj

17 September 1947.

SECRET

MEMORANDUM FOR: Director, L.S.I.C.

(Attention: TICOM).

Subject: Interrogation of Selchow.

1. The attached TICOM report is transmitted herewith for your information. If you consider further interrogation of SELCHOW, I will so inform the authorities at ASA Europe.

William G Bartlett

WILLIAM G. BARTLETT,
Lt. Col., GSC., U.S.Army,
Senior U.S. Liaison Officer.

SECRET

HW 40/181

15(a)

SECRET

APO 757

ASA-13/MCL/ab

3 September 1947

SUBJECT: Interrogation of Selchow

TO: IDWD Detachment
c/o Military Attache
London, England
Naval Fleet Post Office No. 100
(to be passed to TICOM)

1. Pursuant to request of Army Security Agency, Washington for information concerning Selchow of the German Ministry of Foreign Affairs, the inclosed report is forwarded as a preliminary interrogation report of Selchow conducted by a representative of Army Security Agency, Europe at Frankfurt am Main, 2 September 1947.

2. It is requested that this Headquarters be advised whether further interrogation of Selchow is desired by TICOM, and if so, that specific questions be forwarded to this Headquarters for use in the interrogation.

3. A copy of the inclosed report has been forwarded to Army Security Agency, Washington and that Agency has also been requested to advise whether further interrogation is desirable.

Incl
Report of Interrogation

ROBERT T. WALKER
Lt. Colonel, Signal Corps
Chief

SECRET

15(2)

TOP SECRET

TICOM/I-208

INTERROGATION REPORT ON KURT SELCHOW, FORMER HEAD OF THE PERS ZS DEPARTMENT OF THE GERMAN MINISTRY OF FOREIGN AFFAIRS.

Attached is a report on the interrogation of Gesandter Ministerdirigent Kurt SELCHOW, former head of "Pers ZS", the crypto-bureau of the German Ministry of Foreign Affairs, carried out at Frankfurt-am-Main on 2nd September, 1947, by Captain Mary C. LANE of A.S.A. Europe.

2. The report is of general historical interest, and SELCHOW claims to have no technical knowledge. For detailed interrogation report on the work of his department, including the personnel mentioned by him on page 10, see Ticom/I-22.

TICOM
27th October, 1947.

No. of Sheets: 3

Copy No: 11.

Distribution :-

L.S.I.C.

1. T.
2. S.
3. H.
4. Brigadier Tiltman.
5. L.
6. Z.
7. H.71
8. R.1 for Dr. Morgan.
9-10. Z.86.
11. L.91.
12-15. Ticom Files.

U.S.L.O.

16. U.S.L.O.
17-20. Op-20-2.)
21-24. A.S.A. Washington.) via U.S.L.O.
25. Chief, A.S.A. Europe.)

TOP SECRET

INTERROGATION REPORT ON KURT SELCHOW, FORMER HEAD OF THE PERS ZS DEPARTMENT OF THE GERMAN MINISTRY OF FOREIGN AFFAIRS.

Personal Data:

a.	Surname:	SELCHOW.
b.	Christian Names:	Kurt Richard.
c.	Aliases:	None.
d.	Date and Place of Birth:	28 May 1886. Oppeln, Upper Silesia, Germany.
e.	Nationality claimed:	German.
f.	Occupation:	Former head, with rank of Gesandter Ministerdirigent, of Cryptoburcau, German Ministry of Foreign Affairs.
g.	Religion:	Evangelical.
h.	Description:	
	Height:	Approximately 6'2".
	Weight:	Approximately 160 pounds.
	Build:	Thin, tall.
	Face:	Square, grey-blue eyes, glasses.
	Hair:	Slightly grey and thinning.
i.	Last Permanent Address:	Wedel bei Hamburg, Schulauerstrasse 9.
j.	Father:	Hugo SELCHOW, Postdirektor at Oppeln (deceased).
k.	Mother:	--------
l.	Brothers:	--------
m.	Sisters:	--------
n.	Wife:	Erna SELCHOW (geboren Schultz).
o.	Children:	One daughter, Gitta.
p.	Identity documents:	Certificate of identity from Office of Chief of Counsel, Nuernberg. Identification card.

Autobiographical Notes: SELCHOW, Kurt Richard was born 28 May, 1886, in Oppeln, Upper Silesia, Germany, the son of the Postdirektor of Oppeln, Hugo SELCHOW. He was educated in the schools of Oppeln until 1906 when he became a soldier. Assigned at first to the Infantry, he was transferred in 1912 to the Signal Corps (Nachrichten Telegrafen Bataillon) in Frankfurt-an-Oder. He served with the German Army of World War I as a signal officer with the troops. SELCHOW stated that even in the midst of World War I he had pointed out to the Chief Signal Officer that much of the work being done in the German Army Signal Corps belonged properly to the German Ministry of Foreign Affairs because of its diplomatic nature. The Chief

Please turn over

Signal Officer did not agree with this statement and during the war much of the work done by the Army was diplomatic. Directly after World War I, however, SELCHOW entered the German Ministry of Foreign Affairs where he organised the crypto-bureau. He brought with him into the crypto-bureau several soldiers whom he had known during the war, viz: SCHAUFFLER, PASCHKE, ZASTROW, BRANDES, HOFFMANN and KUNZE. He remained head of the crypto-bureau until the defeat of Germany in May, 1945. After the defeat of Germany, SELCHOW remained for two years in the French Zone of Germany at Weiler/Vorarlberg, Swabia.

In mid-April, 1947, SELCHOW moved to Wedel bei Hamburg, British Zone of Germany, where he now lives with his wife and daughter in the house of a relative. He is employed in a merchant firm of a relative in Wedel, and his daughter is employed in a factory owned by a relative in Wedel, His wife is ill. SELCHOW expressed the desire to move with his wife and daughter to the American Zone of Germany, preferably to Marburg where he stated, SCHAUFFLER, PASCHKE and KUNZE now live. He has, however, no means of obtaining the necessary permission of Military Government to come into the American Zone and procure a residence.

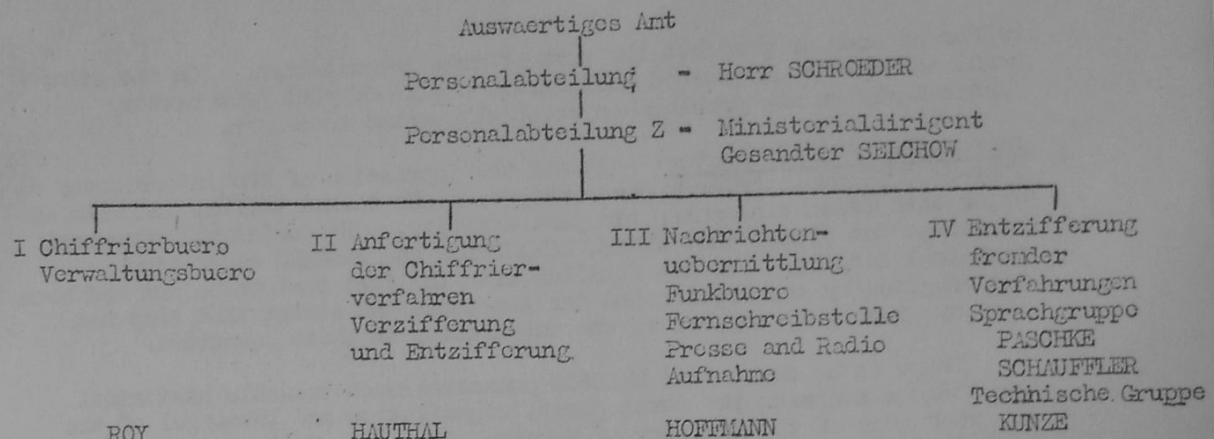
Contact with Foreign Governments since End of War: SELCHOW stated that although he lived for two years in the French Zone of Germany after the end of the war he had not spoken with any French authorities concerning his previous occupation. He stated that when the French had discovered on his identification papers that he had been the head of the Crypto-bureau of the German Ministry of Foreign Affairs they stated that all the crypto-systems had changed and hence they were not interested in questioning him. Once, however, he had learned that for some time it had been thought by the French that his name was a cover-name for a system (the Selchowsysteme). SELCHOW stated that he had never been questioned by the British during his residence in Wedel concerning his previous occupation.

Contact with Former Colleagues: SELCHOW stated that he was in frequent communication by letter with other former members of the German Ministry of Foreign Affairs, particularly those who had been his colleagues during the entire period of his service with the Ministry of Foreign Affairs. As stated above, PASCHKE, SCHAUFFLER and KUNZE were said to be living in Marburg; HOFFMANN, Ernst, Former head of the Funkbuero and Fernschreibstelle of the crypto-bureau was now living in Minden/Westfalien. Dr. HAUTHAL was living at Alten Hohenau/Post Griesstaett/Inn. He stated that Dr. ROY, who had been head of the Verwaltungsbuero of the crypto-bureau had been for some time after the war in a prison camp at Halle/Saale, but was now a prisoner in Russia and had not been heard from for some time.

Notes on History of Crypto-bureau of Ministry of Foreign Affairs: SELCHOW stated that he was familiar with the history of the crypto-bureau of the Ministry of Foreign Affairs from 1919 to 1945. Such a bureau had existed within the Ministry of Foreign Affairs during World War I, but chiefly as an enciphering and encoding group. In 1919, when he became leader of this group, he introduced the system of dividing work upon foreign codes and ciphers into sections for the various countries and selected as leaders of these sections those men such as PASCHKE, KUNZE and SCHAUFFLER who had been known to him during the War. The crypto-bureau had been before 1919 and continued to be throughout World War II subordinated to the Personalabteilung of the Ministry of Foreign Affairs.

The outline of the chain of command within the Ministry and the organisation of the crypto-bureau as he described it is as follows :-

Please turn over



SELCHOW stated that during the latter years of World War II the crypto-bureau of the Ministry of Foreign Affairs had expanded until it comprised between 400 and 500 persons, including both men and women. However, it had up to that time remained relatively small and at the beginning, the group had consisted of only fourteen or fifteen persons.

At the end of the war the crypto-bureau had been forced by bombing to leave Berlin-Dahlem and to move successively southward. This accounted for the presence of SELCHOW near Weiler at the end of the war and for his continued residence in the French Occupied Zone of Germany.

Relation of SELCHOW to OKW/Chi and to the Forschungsamt: SELCHOW was particularly anxious to clear his record of any voluntary relation with the National Socialist Party. He stated that from the very beginning of his diplomatic career he had been interested in a closer co-operation of the various countries of Europe with one another, on something of the same plan now advocated by CHURCHILL. He had not been a militarist, nor had he interested himself in military systems, making it a strict policy within the Ministry of Foreign Affairs that only systems of a diplomatic nature should be dealt with. Until 1933 the crypto-bureau of the Ministry of Foreign Affairs had had the entire field of diplomatic ciphers to itself. The cryptographic systems of the Armed Forces of other countries were handled by the Wehrmacht. With the advent of HITLER, however, the Luftfahrtministerium under GOERING encroached upon the field of the cryptobureau of the Ministry of Foreign Affairs. SELCHOW stated that he himself at this time wished to resign since he had no sympathy whatsoever with the National Socialist movement. He was persuaded to remain, however, by von BULOW who was until 1938 Secretary of the Ministry of Foreign Affairs. Von BULOW, who was also a firm opponent of National Socialism, was extremely anxious that the crypto-bureau of the Ministry of Foreign Affairs remain untarnished by National Socialism and that it be staffed by opponents to the new movement. SELCHOW therefore remained with the crypto-bureau but outside the National Socialist Party until von BULOW's death in 1938. When RIBBENTROP became head of the Ministry of Foreign Affairs a great deal of power was taken from SELCHOW, since von RIBBENTROP did not trust him. His supervisory capacity was restricted to those sections which dealt with the passing of messages to and from missions and to the technicalities of the deciphering of the systems of foreign countries. He was forced to join the Party in 1941 but took no active part in its policy. During the war years he had no exact knowledge of the messages passed and took no part in any matters pertaining to diplomacy.

SELCHOW stated that when he and his colleagues in the crypto-bureau were ordered to collaborate with the personnel of the Forschungsamt, they often gave false information concerning systems or solution of systems in order to

Please turn over

TOP SECRET

hinder as much as possible the work of that organisation. On the other hand, as the war progressed collaboration with OKW/Chi grew better, particularly on new problems on which all worked in common.

Impression of Interrogator: It was the impression of the interrogator that SELCHOW was extremely co-operative. He talked swiftly and with an eager enthusiasm concerning his past activity. He denied all technical knowledge but stated that KUNZE, SCHAUFFLER and PASCHKE could give technical details. He was familiar with the fact that these men had been interrogated by the British and the Americans and stated that they had already given full reports to the authorities in those countries.

There is no doubt that SELCHOW possesses much valuable historical knowledge concerning the development, organisation and personnel of the crypto-bureau of the Ministry of Foreign Affairs. He is evidently in close contact with former members of the crypto-bureau and offered to come to Marburg where PASCHKE, SCHAUFFLER and KUNZE now are and collaborate with them on a complete history of the development, organisation and technical successes of the bureau. He was quite certain that he could also bring HOFFMANN and HAUTHAL into this work, should the United States government wish it. The interrogator stated that this proposal would be referred to the United States government and that he would be informed at Wedel, should further interrogation be required. SELCHOW stated that should he be forced by circumstances to move from his present residence at Schulauerstrasse 9, PASCHKE of Marburg would know where he could be reached.

Staats Sekretaar (Weyacker '39-44 Steengracht 44-45)

Schröder

at end 1943

[Au]swertiges Amt
Pers. Z. S.

Director: Minister 1st. class SELCHOW

Main Dept. - Berlin - Dahlem
ORR. SCHAUFFLER
PASCHKE

SCHAUFFLER
1. Japan
2. Systems & research
3. Applying, experience on foreign cyphers to home systems.

PASCHKE:
1. Admin.
2. Working on & editing of diplomatic tele grams of foreign countries:-

a) Japan, China	ORR.	SCHAUFFLER
b) Turkey	ORR	SCHERSCHMIDT
c) Iran, Afghanistan	RR.	Dr. BENZING
d) Italy, Greece.	ORR.	PASCHKE
e) France, Belgium, Swiss.	RR.	BRANDES
f) Rumania	RR	Dr. KASPER.
g) Yugoslavia		Dr. KRUMMEL
h) U.S.A.		ZASTROW
i) England, Ireland, Spain, Portugal, Latin America.		Frl. HAGEN – Herr Hoffman from 1922 - 1939

3. Information & intelligence card index. — Dr. HORN.

Alternative Station HIRSCHBERG (Rusenjebige)
RR Dr. KARSTIEN

a. Crypto commitments
1. Book building
2. Handling, translation & editing telegrams not of an urgent nature.
3. Current breaking of difficult recyphers.

b. Territories:
a. Bulgaria, Croatia, Poland (RR. Dr. KARSTIEN)
b. Japan, China (Dr. OLBRICHT)
c. Frane, Belgium, Swiss (Frl. SCHRADER)

Staats Sekretär (von Steengracht)
+Ministerial Direktor Schröder — Gesandter Bergmann (held by Russians)

Pers. Z. S. (as at April 1945)

SELCHOW

I
ORR. SCHAUFFLER X

II
ORR. PASCHKE X

III
ORR. Dr. KUNZE X
Mathmatical cryptography.

A. Sections by countries:-

1. France, Belgium, Switzerland Holland.
   Head of Sec: RR BRANDES X
   Deputy: WHA Frl. SCHRADER X
2. Br. Empire, Ireland, Spain. Portugal, Central & South America States, Thailand.
   Head of Sec. WHA Frl. HAGEN X
   Deputy: WHA Frl. WERNICK
3. Italy, Vatican, Greek, USSR
   Head of Sec. ORR PASCHKE X — Iran for Paschke
   Deputy: WHA Dr. DEUBNER X
4. Rumania
   Head of Sec. RR. Dr. KASPER.
   Deputy WHA MENNING
5. Slavonic States (ex. USSR) Esthonia, Lithuania
   Head of Sec. RR Dr. KARSTIEN X
   Deputy WHA Frl FRIEDRICHS X
6. U.S.A. Scandinavia
   Head of Sec. WHA Dr. MUELLER (HANS KURT) X
   Deputy WHA ZASTROW X
7. Turkey — Head: ORR SCHERSCHMIDT X?
8. Iran, Afg anistan Arab States. — Head: RR Dr. BENZING X; Deputy: Frl. Dr. SCHIMMEL
9. Japan, China Manchukuo — Head: ORR SCHAUFFLER; Deputy: Dr. OLBRICHT X

B. Office, information & files. — Head: Prof. Dr. HORN.

Alternative Station HERMSDORF (Riesenjebirge)
ORR Dr. KUNZE

Commitment: Work on difficult crypto problems: Diagnosis and solution of new cypher systems, appearing especially those necessitating largish staff and time or even mechanical equipment.

X= Interrogated.
WHA= Wartime assistant.

TOP SECRET

15(2)

4 NOV 1946

24 October 1946

MEMORANDUM FOR MAJOR E. DALE MARSTON

From Chief ASA-14: As an item of historical interest to TICOM we would like to suggest that the signature SCHAPPER, FIRST LIEUTENANT AND COMMANDER appearing on pp. 20 and 34, inter alia, of D-82, "Camouflaged Secret Writing," a translation of Ticom Document 3294 (Pers ZS papers and correspondence of 1917) is that of Gottfried Schapper, the last head of the Forschungsamt. Schapper gave an autobiography (cf Final Report of TICOM Team 1, Appendix 2) which stated that in 1916-17 he was Director of the Cryptographic Bureau of the High Command of the Army. This identification is considered to be of interest since it affords one of the few checks on the credibility of Schapper. It also suggests the possibility of further questioning of Schapper (believed to be still a prisoner as a former member of the Nazi Party and SS) if warranted as of historical interest for World War I.

Fred Griffin
FRED GRIFFIN

L 91
Your Info
E D Marston

TOP SECRET

15(Q)

Copy to L. 12/10

TICOM/D-81

TOP SECRET

TOP SECRET

CORRESPONDENCE REGARDING THE LACK OF SECURITY OF CRYPTOGRAPHIC SYSTEMS OF THE GERMAN FOREIGN OFFICE.

The attached translation by A.S.A. Washington is of an item from TICOM document T.3297, entitled CRYPTOGRAPHIC ITEMS FROM FILES OF GERMAN FOREIGN OFFICE.

2. The correspondence is dated 1917 and relates in the main to systems supplied to German Naval Attaches by the German Foreign Office and found insecure on examination by the cryptanalysts of the German Naval Staff.

3. Historically this is of interest as an early case of detailed cryptanalytic examination of cryptographic material from a defensive angle.

TICOM
7th October, 1946.

No. of Pages: 11

Copy No: 8

Distribution :-

U.S.G.I.C.

1. T.
2. S.
3. H and M.
4. L.
5. Z.
6. H.71.
7. H.83 for Dr. G.W. Morgan
8. L.91
9-12. Ticom Files.

U.S.

13. U.S.L.O. } via U.S.L.O.
14-17. Op-20-G. }
18-21. A.S.A. Washington. }
22. Director, A.S.A. Europe. }

Ministries

23. Commander Bacon, N.I.D 9., Admiralty.

T 3297.

Your Honor's assertion that almost all cipher telegrams can be deciphered is untenable. If the matter were so easy, the German radio sections would probably not fail to decipher the Russian, English and French radiograms which they intercept. To my knowledge the German radio sections have only succeeded in partially deciphering the Italian radiograms; this may be explained by the fact that they had material supplied by the Austrian-Hungarian army to serve as basis. Without such an aid, the decipherment of unsystematic ciphers is out of the question. That the General Staff is at present not in a position to decipher Russian diplomatic cipher despatches, is best shown by the fact that Major Nicolai recently requested that we turn over our Russian cipher material and the Communications Officer in the General Staff of the Field Army recently repeated this request.

In the case of ciphers of the Foreign Office a distinction must be made between antiquated and new ciphers. Of the former there are usually one or two copies in each mission for the transmission of unimportant reports or identical messages, or - since these are already compromised - for sending out misleading information. In radio communication with Spain, for instance, several bogus telegrams have been sent in a cipher known to our enemies. That the decipherment of such radiograms causes no difficulty is clear. It is different with telegrams enciphered in the unsystematic secret ciphers of the Foreign Office, especially when used with constantly changing keys. Decipherment of these telegrams is simply impossible even for the most clever specialists. It can only result if the entire cipher is betrayed or essential parts and keys come to the knowledge of a foreign government. Of course, there is no absolute security against betrayal and the only aid is the frequent change of cipher and of keys, which is abundantly provided for here.

During the war the Foreign Office has had radio communication chiefly with the embassies in Madrid and Washington and with the mission in Persia. The embassy in Madrid has independently and constantly safeguarded its ciphers by the most intricate systems. However, since the cipher itself could not be changed during the war, it is conceivable, though highly improbable, that radiograms to Madrid could in part be deciphered, always assuming that the literal key employed was betrayed.

For Persia too a secret key is employed for important telegrams. The radiograms to Washington could be read by our enemies since they had to be enciphered with a cipher which is in the hands of the American censors in Tuckerton and Eilvese. Perhaps the observations of the General Staff are based in the main on these telegrams. It would interest me, however, to be informed of these observations in detail.

In my conversation with Major Nicolai he requested the sending of a representative of the Foreign Office to a conference which should discuss an exchange of information regarding cipher material of hostile states now in the hands of the Admiralty Staff, General Staff and Foreign Office. In this way

the decipherment of foreign enciphered correspondence should be furthered so far as possible and at the same time our own cipher system be benefitted. The representative of this office did not give any assurance regarding the turning over of used German ciphers of the Foreign Office for the purpose mentioned by Your Honor and, therefore, could not take back that assurance. Instead, the Communications Officer, Capt. Grabau, was informed that it would be well to turn over to the Foreign Office the intercepted radiograms between St. Petersburg and Russian diplomatic missions abroad, since the Cipher Bureau - on the basis of the older Russian cipher material at its disposal and its long experience deciphering Russian cipher telegrams - might be in a position to decipher them, whereas this was simply impossible for the General Staff. Your Honor will bring up this suggestion most emphatically with the appropriate office.

Our representative expressed himself in general terms at the above mentioned conference respecting the cipher systems used in the Foreign Office and the measures taken for their security. The Foreign Office itself has the utmost interest in safeguarding its telegraphic traffic.

I will say further that in the past year word came from Holland - word which has been repeated several times - that all German cipher telegrams were being read by especially clever enemy agents. Thereupon, 12 sample postal ciphers were given the representative supplying the information, these he was supposed to be able to get into the hands of the agents and also to learn what results they had with decipherment. To date no report on this matter has been received. This shows the value of such reports.

I leave it to Your Honor to use the foregoing in friendly fashion in the proper quarter. I have not the slightest doubt of the loyalty of the Army Supreme Command in the question.

Representative of the Foreign Office
at Grand Headquarters Nr. 158, Secret.
General Headquarters, 23.III.17.

I bring to Your Honor's attention the foregoing letter of the Secretary of State of the Foreign Office to me. Please treat as confidential.

(Signed) Baron V. Lersner

TOP SECRET

Chief of the Admiralty Staff of the Navy
II

Berlin, 14 April 1917.

Very Secret.

Persuant to my letter D 2584 II of 22 March I have had the codes of the Foreign Office Nr. 200, 604, 2505, and 1303 which were turned over to the Navy subjected to a brief examination. The result of this examination which is enclosed, has convinced me that these codes are not suitable to guarantee adequate security over any considerable period of time. I have therefore ordered their withdrawal from all Naval Offices (attaches) at present supplied therewith.

Signed Signature

To Imperial Privy Counsellor, Secretary of State of the Foreign Office, Mr. Zimmermann, Excellency, Berlin.

Chief of the Admiralty Staff
of the Navy
D 2908 II.

Berlin, 14 April 1917.

Very Secret.

To the Royal Field Marshall General, Chief of the General Staff of the Field Army, Mr. von Beneckendorff and von Hindenburg, Excellency, Grand Headquarters.

Enclosed I send Your Excellency for your information a copy of a letter to the Secretary of State of the Foreign Office.

Even though it is impossible to judge here whether the other secret means of communication used by the Foreign Office afford greater security, the results of the investigation of four codes turned over to the Navy during the course of the war for its use - which therefore were evidently regarded by the Foreign Office as sufficiently secure - make it imperative to use caution in transmitting secret material through the mediation of the Foreign Office.

(Signed) von Holtzendorff

Chief of the General Staff of the
Field Army
I C Nr. 3119 Secret

Grand Headquarters
7 May 1917.

Only by Officer.

Through the letter of the Chief of the Admiralty Staff D 2908 II of 14 IV it has come to my attention that individual secret codes of the Foreign Office are not absolutely secure.

Should this be true, I request, that a suitable draft of a letter to the Foreign Office be prepared for me.

I enclose the material at hand for your confidential use.

By Order
Ludendorff

5 enclosures

TOP SECRET

TOP SECRET

To the Chief of Field Telegraphy.

Chief of Field Telegraphy
Grand Headquarters. Received: 7 May 1917.
Section IV Nr. 4941 Secret.

Sent 10 May 1917 with a draft.

Chief of General Staff of the Field Army 10 May 1917
Chief of Field Telegraphy
Section IV Nr. 4941 Secret

To I C Nr. 3119 Secret of 7 V 17
Re: Security of the Codes of the Foreign Office.

To Chief of the General Staff of the Field Army.

I agree with the view of the Chief of the Admiralty Staff of the Navy. The requested draft of a letter to the Foreign Office is enclosed.

On behalf of the Chief of Field Telegraphy

1 enclosure. (Signed) von Massow.

DRAFT

Through a letter of the Admiralty Staff of the Navy I am made acquainted with the fact that four systems of secret communication supplied by the Foreign Office during the course of the war have not proven adequately secure. The Admiralty Staff has found itself forced to order the withdrawal of these codes from all Naval offices (attaches) equipped therewith.

The fact that these codes were furnished to the Navy for use during the war leads to the conclusion that the codes of the Foreign Office are composed on the same principles and therefore do not afford adequate security.

In view of the extraordinary importance which the security of the codes of the Foreign Office has for the collective interests of the nation, I can not fail to suggest once again to Your Excellency subjecting the codes used by the Foreign Office to an examination by experts who had no part in the production of these codes.

The art of decipherment has developed into a science during the war.

Under the Chief of Field Telegraphy there is an office which is exclusively occupied with the decipherment of foreign systems and which has succeeded in breaking nearly all field and naval systems now in use as well as several diplomatic systems. Even unsystematic ciphers with changing decipherment have been solved by this office without any aid from other sources.

I propose therefore that Your Excellency utilize the rich

experience of this office and have the codes in question checked by an officer of this office. Details could be arranged with the Chief of Field Telegraphy.

Chief of the Admiralty Staff of the Navy
3749 II

Berlin, 28 VII 1917

Very Secret.

In connection with D 2980 II of 13 April (I beg to inform you) that for special reasons the telegraphic communications of the Foreign Office with the Imperial Embassy in Madrid has been subjected to a study of its security. This investigation has confirmed the previous opinion respecting the codes constructed on the model of 2505, inasmuch as all enciphered telegrams could be deciphered in 14 days. With respect to the so-called Lotterie Cipher employed for more important matters, investigation showed that this did indeed involve greater difficulty in solution but nevertheless would only assure adequate security if certain defects were eliminated and if a number of codes were available for use at the same time.

(Signed) von Holtzendorff

To the Royal Prussian Field Marshal General,
Chief of the General Staff of the Field Army
Mr. von Beneckendorff and Hindenburg,
Excellency,

Grand Headquarters.

R. Chief of Communications
with request for opinion.

by order
B. L.

Chief of the Communications Service Grand Headquarters 1 VIII 17.
Section IV f Nr. 7428/4 Secret

I agree with the view of the Admiralty Staff. Here too traffic of the Foreign Office with Madrid is intercepted and worked on. One of the codes used between the "Minister of Foreign Affairs" Berlin and Madrid was solved after 14 days. The Chief of the Communications Service made personal report of this to the Quartermaster General. Telegrams from this traffic are enclosed.

A check of the codes of the Foreign Office for solubility by experts is considered absolutely essential, as already reported.

By Lotterie Cipher is understood a code in which the groups are not arranged in alphabetical order but distributed in random fashion after the manner of a lottery.

V. S. d Ch. d. N.
U. Ch. d. G.
(Signed) von Massow

TOP SECRET

Foreign Office
Ch. B. 768
J Nr. 18931
11 enclosures

Berlin, 11 August 1917.

Very Secret.

I am returning to Your Excellency the telegrams enclosed with your letter of 6th inst. M. J. Nr. 21625 with the obedient remark that they did not originate with the Foreign Office but from the Admiralty Staff, or were destined for the latter, and that they are enciphered with the Naval communications book and the Naval keys. Only the beginning of Tel. Nr. 26 of 2 March (Sheet 6) is given in a cipher of the Foreign Office and not enciphered.

I leave it your judgment whether to inform the Chief of the Admiralty Staff of the foregoing.

So far as the decipherment by the Admiralty Staff of the telegrams of the Foreign Office enciphered after the model of the antiquated code 2505 is concerned, it may be remarked that this was only possible due to the exact knowledge of the Foreign Office cipher material available at the Admiralty Staff and on the basis of actual decipherments of telegrams supplied from here since sent for that department. Decipherment of telegrams in the Lotterie Cipher has not yet been undertaken by the Admiralty Staff here.

The Foreign Office adheres, first and last, to the point of view that its new Lotterie Ciphers, especially when reenciphered, can only be regarded as not absolutely secure if betrayal or careless use of the ciphers or of the enciphered correspondence occurs.

(Signed) Signature.

To the First Quartermaster General,
General of Infantry,
Mr. Ludendorff, Excellency,
Grand Headquarters.

Chief of the General Staff of the
Field Army
I C Nr. 4291 Secret
R. Chief of Communications

14 VIII 17

Reference your IV f Nr. 74284 secret with request for opinion.

by order and acting

(Signed) von Bockelberg.

T O P S E C R E T

Copy.
Ch. B. 750
J Nr. 19342
Very Secret

Berlin, 17 VIII 1917

In reply to letter of 27th ult.
D. 3749 II

With the intimate service relations which have always obtained between the Admiralty Staff and the Foreign Office the latter has never hesitated to place at the disposal of the Admiralty Staff its cipher material, just as the Admiralty Staff has turned over its codes (Traffic and despatch books) to the Foreign Office. In this way the Admiralty Staff gained insight into our cipher systems. Since the land line communication with Spain has been blocked all telegrams of the Foreign Office to and from Spain have passed through the war central office of the Admiralty Staff. Telegrams arriving here from Madrid, which are destined for the Admiralty Staff, have hitherto been passed on to the latter in clear without any change so that both cipher text and plaintext were available together. Even new keys have been sent from Madrid in Naval code. Thus, the opportunity for decipherment was provided. Under like circumstances other codes could be read too.

In the telegram decipherments submitted the Lotterie Cipher was not employed in a single case. The Foreign Office therefore sticks to the point of view that its new Lotterie codes are perfectly secure provided no possibility of unauthorized decipherment is given by betrayal or lack of caution in their use.

In judging the Madrid Ciphers consideration must be given to the unavoidable circumstance that they could not be changed during the war, otherwise the series to which 2505 belongs would have been replaced long since by the Lotterie Cipher. As stop-gap serve the variations of the ciphers used by Madrid, these changes are frequent and, in part, very serviceable. For instance the system of the Naval codes with slidable, frequently changing keys is used there.

For the rest, we are working unceasingly to attain the utmost possible security of our enciphered correspondence by frequent change of codes and recipherments.

(Signed) Kuehlmann

To the Chief of the Admiralty Staff of the Navy.

Ch. B. 960 25 IX 17 Grand Headquarters of His Majesty,
Chief of the Communications Service 23 IX 17.
Section V Nr. 79141

To the Chief of the General Staff of the Field Army.

Enclosed are enciphered radiograms of a circuit Koenigwusterhausen - Madrid which have been solved by my evaluation center in Grand Headquarters. It appears to be a question of a secret traffic of the Foreign Office in Berlin with its representatives in Spain.

T O P S E C R E T

It is requested that one ascertain whether the solved messages agree with the originals.

13 enclosures (Signed) Hesse

U. R. Secretary of State of the Foreign Office with a request for prompt statement.

(Signed) Ludendorff.

U. Chief of Communications Service

Foreign Office informs that the Cipher Service of the Foreign Office is being reorganized.

(Signed) von Bartenwerffer 8 X.

Radio Section Grand Headquarters of His Majesty 22 IX 19.7
O.H.L. (A.)
D. 468

Result of Investigation of Cryptographic Systems used in Radio Traffic between Berlin and Madrid

The various types of radiograms observed here in traffic lp - ego, signed on the one hand by Zimmermann, Kuehlmann, Stumm, Bussche and on the other hand by Retibor, Bassewitz, hence beyond doubt belonging to the telegraphic communications of the Foreign Office with the Imperial Ambassador Prince Ratibor in Madrid, can be divided essentially into two main groups:

1. Telegrams which have at the beginning the indicator groups 27082, 18470, 21894, 1777, 12444 with 4 and 5 digit groups up to 30900 and rare groups above 30900.

2. Cipher telegrams with the indicator groups 0053, 5003, 5300, 0000, 4343, 1357, chiefly with 4 digit groups.

The investigations were made on the basis of intercepted radiograms, i.e., with the same means which - at the very least - would be available to an unauthorized, hostile decipherer.

The results are as follows:

To 1. Work on telelgrams with indicator group 27082 showed that:

a. the telegrams are encoded but not enciphered.

b. the code used is systematic; the code groups are composed of 2 and 3 place heading numbers and 2 place column numbers. Groups with the same heading number lie near together in the alphabet.

Since there is no doubt about the possibility of solving an unenciphered systematic code, and since furthermore from a solved cipher telegram the relationship of the systems 27082, 21894, 1777, 12444 was evident, work was not carried further with these systems. (Cf. Radiograms read - Supplements 11 and12).

T O P S E C R E T

Chief of Communications Service
Section IV f Nr. 7428⁴
In: 14 VIII out 17 VIII 17

It was assumed here that the traffic with the inscription "Minister of Foreign Affairs Madrid" and "Minister of Foreign Affairs Berlin" was conducted by the Foreign Office or at least enciphered there. From the above communication from the Foreign Office, as well as from solution of another system in this traffic which has been made meanwhile (Political Section O.H.L.) it appears that this is not the case. The various, as yet unsolved systems from this traffic, among which that of the Foreign Office must be found, are being worked on further.

11 enclosures.

V. S. d. Ch. D. N.
d. Ch. d. G.
(Signed) von Massow

Foreign Office
Ch. B. 545
J. Nr. 19241
In reply to letter of 11 May of this year.
I C Nr. 3119 Secret
1 enclosure
Very Secret

Berlin, 17 August 1917

Representative of the Foreign Office in Grand Headquarters
Nr. 654
through: 19 VIII 17
signed Baron von Lersner

Your Excellency's assumption that the ciphers assigned to the Navy were considered by this office to be sufficiently secure, is correct. The Foreign Office still takes the point of view that the other ciphers too - especially the Lotterie Ciphers with recipherment according to new principles, are absolutely secure so long as there is no betrayal or careless handling of cipher material or enciphered correspondence. Too long a use of the code is, of course, likely to shake faith in the code and we have always taken care to change codes and keys frequently. Unfortunately it has never been possible to change the frequently used codes in Madrid as we should have liked, due to the war, however frequent change in encipherment has been made.

To the statements of the Admiralty Staff regarding decipherments of telegrams of the Foreign Office to and from Madrid, I have stated my position in my answer of 17th inst., and have the honor to send Your Excellency a copy herewith.

Copy of Ch. B. 750

(Signed) von Kuehlmann

To the First Quartermaster General,
General of Infantry,
Mr. Ludendorff, Excellency.

TOP SECRET

To 2. Investigation of the telegrams with indicator groups 0053, 0000, 4343, 1357 yielded the following results:

a. the telegrams encoded with a code and enciphered by several methods. In 0000 encipherment is by simple transposition of the digits of the groups, in the other telegrams by addition and substitution according to frequently changing keys. (Supplement 1)

The discovery of the types of encipherment and thus the reduction of all these types to one basic type was carried out by one operator in 3 weeks.

b. The code thus discovered is entirely 4 place; the fifth digit prefixed to many groups is a blind. No system was found in the structure of the code. The code turned out to be the completely irregular so-called "Lotteriechiffre". Contrary to the opinion of the Foreign Office which "adheres first and last to the view that the decipherment of the Lotteriechiffre is absolutely impossible" two workers were able in 4 weeks to reach the state of decipherment shown in the appended telegrams (Supplements 2 - 10). According to our experience with other Lotteriechiffres in diplomatic traffic (e.g., Italian K. 19) it would be possible in a few weeks to carry the work to a point where almost every telegram could be solved for practical purposes.

The preceding proves that system 0053, 0000, 4343, 1357 can be solved and is therefore open to criticism.

Regarding the appended solutions of messages it may be said that:

1. The 3 place groups in the heading generally show number and date of the message. These are enciphered by a special table for numbers and dates which was solved here.

2. It lies in the nature of a non-alphabetic code (Lotteriechiffre) that the recovered values of cipher groups do not always agree in wording with the meadings in the original code and that words or rare occurrence can only be deciphered with limited certainty.

I. V.
(Signed) Stuetzel
Lt. of the Reserve.

15(Q)

TICOM/D-78

TOP SECRET

19

B

PROPOSED COLLABORATION BETWEEN GERMAN FOREIGN OFFICE AND ARMY

The attached translation from Ticom document T.165 was received from A.S.A. Washington.

2. T.165, from the files of Section Pers Z.S. of the German Foreign Office, consists of Diplomatic Memos (1944) on proposed joint working by the German Foreign Office and Army on Russian Cyphers.

Ticom
30th September, 1946.

No. of Pages: 4

Copy No: 9.

Distribution:-

L.S.I.C.

1. T
2. S
3. H and M
4. L
5. Z
6. H.71
7. H.62
8. H.63 for Dr. G.W. Morgan
9. L.91
10-13. Ticom Files

U.S.

14. U.S.L.O. } via U.S.L.O.
15-18. Op-20-G } via U.S.L.O.
19-22. A.S.A. } via U.S.L.O.
23. Director, A.S.A. Europe } via U.S.L.O.

T O P S E C R E T

T. 165. (Proposed Collaboration between Foreign Office and Defense)

Berlin 23 II 34.

My dear Mr. Superior Government Counsellor:

One could begin with the taking over of our F 65 (328) Monday if you find the following lines acceptable.

For the present we could be ready for this purpose Monday, Tuesday, and Wednesday from 3:45 to 6:00 p.m.

Respecting the other numbers 49, 50, 53, 54, I shall phone you further suggestions early on Monday.

Respectfully yours

Dr. Müller

On 19 II Capt. Oschmann called on me to talk over with me technical details concerned in (our proposed) collaboration.

In the course of the conversation he mentioned an utterance by his chief, Corvette Capt. Patzig to the effect that all cryptanalytic connections with F.A. should be dropped since Cryptanalytic work did not belong in the province of F.A.

Details of the collaboration were then drawn up in broad outline.

Berlin, 19 Feb. 1934

Draft.

This forenoon Capt. Oschmann, Prof. Nowopaschenny, and ORR Fenner of the cipherbureau of the Reichswehr (Defense) came to the ((Foreign)) Office to talk over the possibilities of technical cryptographic cooperation in the field of Russian ciphers.

To my great disappointment I learned that the gentlemen from the Reichswehr were not able to give any suggestions whatsoever in the field of Russian ciphers and that since 1930, when I last talked with them, they had had absolutely no success with Russian ciphers on foreign circuits. Mr. Fenner summed this up with the words: "Completely blank." The Reichswehr has only worked on Russian army, navy and GPU ciphers employed in internal radio traffic and intercepted here. This material has not been available to us; it has been sent us only in exceptional cases, evidently by mistake. The work of the Reichswehr on this material has yielded practical results. Prof. Nowopaschenny informed me briefly that for cipher messages of the GPU in internal traffic a 3-place code is used, the first and second positions are reciphered with changing substitution tables while position c (3rd) remains unreciphered. I got no significant information today regarding military or naval systems and it will be in the interest of our work to obtain some description of these systems from the gentlemen of the Reichswehr when we have another meeting. I gave Mr. Nowopaschenny and Mr. Fenner the general outlines of Russian ciphers. I pointed out that there is a great similarity of system between the ciphers used by the several Russian departments.

T O P S E C R E T

Everywhere there are systematic codes and extensive additive recipherments. I recommended working in the field of least resistance and made the following concrete proposal: To study fully in a statistical fashion the Strahlen-Verfahren (ray-system) Wn. Bl. A. 1. in use between Berlin and Moscow up to 31 Dec. 1930 while the 5-place Wn. T. C. II. was still employed and on which many preliminary studies are at hand. I hope through such statistics to be able to investigate the Tritheims already discovered with regard to further occurrences, i.e. to determine whether the quota of repeats of the Tritheim lies higher than 2 or 3. I showed the gentlemen from the Reichswehr the strikingly frequent repeats of the Tritheim keys and handed Prof. Nowopaschenny 26 sheets with the "Tritheim fragments" of Wn. Bl. A. He promised to have these sheets copied as quickly as possible and to send me a copy.

(Signed) Paschke.

In a conversation between Capt. Oschmann, Capt. Weiss, and myself in the R. W. M. on 12 II 34 the following suggestions for collaboration by the cipher sections of the army and the Foreign Office were made in view of a possible mobilization: Exchange of experiences and greatest possible cooperation in the field of

1. intelligence technique
2. cryptanalysis
3. our own cryptographic service.

Re 1.: To assure undisturbed communication with offices abroad both the A. A. (Foreign Office) and R. W. M. (Reichswehrministerium) should work to set up radio communication agencies quite independent of foreign means of communication.

In the A. A. this should include advising the missions in the procurement of commercial broadcast receivers and as far as possible supplying the same from the central office.

The R. W. M. on the other hand lays special emphasis a priori on setting up in at least part of the places apparatus which will ensure the widest possible telegraphic reception and for very special occasional purposes a potential, camouflaged sending station. Insofar as military attaches are stationed with missions the R. W. M. would, in agreement with the A. A., equip such receiver/sender stations and supply the attache a technically trained man to operate the same. In the opinion of the R. W. M. it would be most useful for the A. A. to equip other posts with such apparatus and to supply a civilian operator.

Re 2.: Since the traffic of the European countries is worked on by R. W. M. in preparation for any possible emergency and by the A. A. for current information, closer cooperation in this field was decided on. In the interest of the most rapid possible increase in production and to avoid duplication it is the intention--after exchange of information on the present status of the work of both parties--to make a division of work on current systems and to form common workgroups for the unsolved political and military systems, on which the A. A. in particular has not

been able to work due to lack of personnel. Details are to be settled in conferences of the section heads.
Re 3.: Since the army with its military attaches is dependent for transmission of its reports upon the cipher systems of the A. A., it has a departmental interest in the security of the diplomatic systems. It was suggested that close cooperation would be in the mutual interest in the matter of defense against foreign interference, in exchange of agent's information on the subject and regarding breaches of security in the handling of the ciphers.

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

TICOM/I-172 retained under S3(4) of the PRA 1958

(date) 11/2/2004

(Signed)

OFFICES OF THE CYPHER POLICY BOARD,
C/o ROOM 17,
FOREIGN OFFICE, S.W.1.

15(Q) 17

10, CHESTERFIELD STREET,
LONDON, W.1.
GROSVENOR 3095-6

TOP SECRET

Ref. 89J/1983 28th September, 1945.

Dear Dudley,

Herewith two copies each of interrogations of Fraulein Hagen and O.R.R. Paschke.

I have not copied your questionnaire for Hagen as I take it you have retained a carbon. I assume also that you will arrange for any necessary circulation by the Ticom Committee.

Yours sincerely,

Cdr. (S) R. Dudley Smith, R.N.
Station 'X.'

Encs.

Issued as 1

Reports

3.12.

PUBLIC RECORD OFFICE

Group/Class ..... HW 40

Piece 181

Interrogation of Fräulein Hagen retained under S3(4) of the ~~PRA~~ 1958

(date) 11/2/2004

(Signed) .....

Interrogation of O.R.R. Adolf Paschke, (Berlin-Wilmersdorf, Johannisbergerstrasse 17a) of Pers ZS, by Commander Bull, R.N.V.R., at Military Government Offices, Marburg Lahn, Germany, 13th September, 1945.

(16)

1. Paschke worked as a cryptographer for the German Army 1915 - 1919. Joined Pers ZS 1919. Joined Nazi Party 1933.

2. Selchow (Director Pers ZS) as a rule dealt direct with Ribbentrop and did not go through Schroder and/or Weisszacker.

3. The instructions from Ribbentrop were invariably of a general nature and solely concerned with the subject matter of intelligence - e.g. Poland - or the invasion. He did not concern himself with the details of different systems in any way.

4. Ribbentrop was well aware that the more important intelligence could only be gained from attacking the recyphered systems, but he was apparently satisfied not to press for the additional staff which would be required and contented himself with the material obtained from the single process codes.

7. They worked on all traffic - Embassies, Legations and Consulates.

8. He thinks the O.K.M. had the biggest staff - about 400. None of the other bureaux had more than 300.

9. Ribbentrop only read about 20% or 30% of the material produced. His secretaries, e.g. Herr Weber and Herr Loesch selected these for him.

10. F.A. read I.D. for a short time in summer 1941.

11. Ministerialrat Fenner (believed in Bavaria) (in 1944 M.R. Wendland assisted him) - held the same position in O.K.W. as Paschke in Pers ZS and was a good friend of his, both being born in St. Petersburg. His (Fenner's) immediate chief was Oberst Kettler and his (Kettler's) was General Gimmler, then Keitel.

12. In F.A. Ministerialdirigent Schroder held the corresponding position to Paschke. Ministerialdirektor Schapper was above him and then Goering.

13. The German secret cypher systems Paschke believed to be first class.

14. O.R.R. Langlotz was head of department of Auswertiges Amt dealing with German cyphers.

15. In 1944 O.K.W. (Fenner) took over the organisation of O.K.M., O.K.L. and O.K.H. cypher construction.

16. Paschke considers that of the three high AA officials

/ [illegible]

concerned with diplomatic traffic von Ribbentrop took most interest as had von Neurath before him. The most interested of all was von Rathenau (1922).

17. The reading of code telegrams besides giving occasional 'highlights' provided a wealth of press material not otherwise available.

18. The Staatssekretar decided on the distribution of telegrams in the A.A.

19. All the Pers ZS papers (40 chests) believed to have gone south to Bavaria from Muhlhaus in mid-April 1945. There were no other copies left.

20. Individual texts bore no marking but the files and folders were marked Geheime Reichssache.

21. No attack was ever attempted on British Attache Cyphers. They were considered O.K.W.'s "pigeon."

22. Paschke was in practice the "Cypher Security" Adviser for the A.A.

23. Frau Paschke worked in Dr. Paschke's section for three years, but only as a clerk. She has never been asked by the Russians (from whom she obtains permits to visit Paschke from Berlin to Marburg) what she did or what her husband's profession was. Paschke enquired as to the possibility of the British providing air transport for Frau Paschke to join him at Marburg.

15(Q)

Copy ordered for H.C.S.C. Sent 23/11 20/11

TOP SECRET

TICOM/D-23

TRANSLATION OF THREE REPORTS CONCERNING COMMUNICATIONS FROM THE PERS. Z.S. ARCHIVES

Attached are translations made at A.S.A WASHINGTON of three documents from captured archives of Section Pers. Z.S. of German Foreign Office at BURGSCHEIDUNGEN.

(a) Short general report on high-speed morse and the wireless teleprinter ((Hellschreiber)).

(b) Historical report on the development of the Morse Code by Assistant PAULA MUELLER.

(c) Communication dealing with use of Enigma cypher machine addressed by Amt Ausl.Abw. to German Foreign Office for attention of Reg.Rat.HOFFMANN, dated 5/12/40.

(TICOM Docs. Nos.380 and 16).

TICOM

No. of Pages: 13

30th October, 1945

DISTRIBUTION

British

D.D.I
H.C.G.
D.D.(N.S.)
D.D.(M.W)
D.D.(A.S.)
C.C.R.
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (2) (via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET (via Lt. Col. Johnson)
Col.Kunkel, USSTAF

TICOM

Chairman
S.A.C.
Cdr. Bacon
Lt. Col. Johnson
Major Seaman
Lt. Cdr. Manson
Major Cowan
Capt. King
Ticom Files (4)

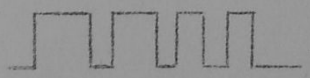
Additional

Mr. Twinn
D.D.(A)
A.D.(W.T.C.)

Notes on Modern Wireless Receiving Apparatus

For receiving messages sent out, there are available today a number of instruments all functioning on more or less like principles. If it is a question of taking Morse characters at a speed up to 175 a minute, then it is generally by headphone and typewriter. The German telegraphers send their Morse at any average of 25 words, i.e. 125 letters per minute since a word averages 5 letters. English and American stations work at a speed of 30 to 35 words, i.e. up to 175 letters per minute. Since auditory reception usually runs for hours at a time and may be rendered very difficult by local disturbances, fading, or jamming, it naturally calls for a great amount of practice and great concentration.

At a speed of more than 175 letters per minute, such as is attained with mechanical transmitters, in simple cases a Morse printer is used or better yet a lever writer /Hebelschreiber/ or recorder devised especially for this purpose and successfully employed for years in commercial communication. The principle of operation is briefly: In the field of a powerful electric magnet is suspended in vertical position by two thin wires a revolving coil to which the impulses are conducted when received, amplified and rectified by the radio receiver. At the upper end is a small, horizontal silver tube one end of which is immersed in a small inkwell while the other end traces a colored line on a paper tape which is moved past by a motor. As this coil receives short or long impulses it is diverted from its rest position to one side and the tube traces the impulses in a jagged line. The letter Z would, for instance, appear as follows:



Such a device, given good conditions for reception, permits of a speed up to 1250 letters per minute.

In recent years another instrument has become increasingly important. This is the Morse-printer of Siemens-Hall which prints Morse symbols as follows:

/Line of tape -- no sample available./

Its advantages are: simple, sturdy construction and relatively simple operational attention. Speed attained is about 1500 letters (300 words) a minute.

A special model of this machine receives as high as 2500 letters a minute. This performance is attained by making the movable anchor of the magnet very light and cutting the motion to a few tenths of a millimeter.

It has long been the ambition of technicians and engineers to build a machine which would permit direct transmission of the printed letter by radio as the teletype does by cable. To date the only machine giving tolerable results when reception conditions are good is the SH-Hellschreiber /teleprinter/ invented by graduate engineer Dr. Hell some time ago and constantly improved. It permits a speed of 300 words a minute.

Formation of the characters is as follows: The radio receiver amplifies and rectifies the impulses received. When such an impulse comes in, the receiving magnet attracts its anchor, the edge of which presses a paper tape, which moves at uniform speed, against the writing spiral which is mounted on a rapidly revolving cylinder and inked by a felt inking roll. Thus there is printed on the tape a vertical stroke with interruptions corresponding to pauses between impulses, which together yield the form of the letters which appear as follows:

One may, therefore, regard the Hell-system as a simple transmission of the printed letter by facsimile.

****

Translated by Dr. Ray W. Pettengill
10 August 1945

15-7-44
Ticom 380

TOP SECRET

S.F.B. Morse and the Morse Code

by Assistant Paula Mueller (née Rhode)

A. Historical Survey.

The Morse code is a system of symbols serving for transmission of information by electric current, light, etc. Knowledge of it is useful not merely for radio and telegraph operators, etc., but for everyone who has much to do with telegrams, chiefly because this will give clues for correcting garbles.

In olden times people relied on swift courier service, then sound and light signals were employed. The fact that water conducts sound better than air was known in Aristotle's day (ca. 500 B.C.) so that it is likely that underwater signals were used at that time.

Not until recent times do we find purely technical solutions of the problem of speeding news from place to place. The best known arrangement is the telegraph introduced by the Frenchman Chappe in 1793 under Napoleon. This involved light signals at night and shadows by day. While it has been calculated that the torch telegraph communication of the Greeks could send up to 173 signals in a half hour, Chappe's telegraph required only 11 minutes for the same number of signals. With later improvements, in particular in the form used in 1813 in Prussia on the line Berlin - Coblenz, this speed was materially increased. The distance between the individual telegraphs (the position of the arms and beams was observed by telescope) averaged 14 km. Some idea of the value of the telegraph service of those days may be gained from the fact that a signal took only two minutes to travel from Paris to Lille (200 km).

Chappe's telegraph brings to an end an epoch characterized by imperfect, time consuming transmission of news. But even though the speed of Chapee's telegraph was great for his day, its general use was impossible due to costs. Since at least two officials had to be present at every relay station, a telegram from Berlin to Coblenz required the activity of 122 officials, an outlay which very few telegrams would seem to justify, and which was all the more a luxury since only for a few hours of the day was visibility adequate for reading the pointer positions. It is interesting, however, that Chappe's telegraph is still used on railroads and for regulating traffic.

Chappe's telegraph in its various transformations was the direct precursor of the electric telegraph. With electricity the bearer of the news becomes a medium which moves with tremendous speed compared to the light waves previously employed, and with a range which, compared again to light, is virtually unlimited.

The first electric telegraph writing permanent symbols was put in operation in Munich in 1837 by Steinheil. In that same year Morse made a preliminary announcement concerning his invention to the United States Patent Office.

To Morse belongs the credit for having so far developed his invention that due to its advantages it could win world wide acceptance. In the Morse telegraph electric impulses of longer or shorter duration call forth corresponding movements of the anchor of an electric-magnet; these movements activate the writing lever which writes characters in shorter or longer strokes on a paper tape which is moved past at uniform speed.

B. The Structure of the Morse Alphabet.

To Morse we owe a carefully thought out arrangement of such short and long telegraphic elements (impulses) to form an alphabet which has now found international recognition. On the paper these elements appear as short and long black strokes separated by white intervals. The short stroke is the unit of length and is termed "dot" /Punkt/. The long stroke is thrice as long and is termed "dash" /Strich/ Dot and dash are the elements.

The pause between the elements of a Morse signal has the length of one unit (one dot); the pause between the Morse letters of a word has the length of three units; the pause between two words the length of five units. (In our representations these lengths have not been observed exactly.)

The black unit of length (dot) and the white unit of length we call the "basic elements" /Grundelemente/.

A Morse text can be represented as a dyadic sequence of the two basic elements: if we call the white element 0 and the black 1, the Morse text

. _ . . . . . _ _ . . .

r e i s e a b

takes the form: 10111010001010011100010111001110101

r e i s e a b

Dyadic sequences of various types play an important role in mathematics and cryptology.

A second manner of representing a Morse text by zeros and ones would be to represent the dots by 0, the dashes by 1, leaving the intervals between elements and words as graphic intervals:

010	0	00	000	0	01	1000
r	e	i	s	e	a	b

But this is no longer a dyadic text, rather we must conceive it as a 30-adic text. The text elements are the 30 variations of 1 - 4 zeros and ones.

In table 1 the Morse alphabet is given in its present form. As a matter of principle in the Morse alphabet the most frequent letters are represented by the shortest symbols. Table 1 contains in addition to the 26 letters of our alphabet ä, ö, ü, ch, thus exhausting the 30 Morse symbols with 1 - 4 elements.

In table 2 the Morse alphabet (without ä, ö, ü) is represented by mnemonic words. These are intended to facilitate memorizing the Morse letters. The first letter of the word corresponds to the letter, the number of syllables to the number of dots and dashes, each syllable with "a" is a dot, any other vowel means a dash. For the letters j, q, y, ö note the word jyqö: In the Morse symbols for these the dot moves ahead corresponding to the position of the letters in the word:

j = · – – –

y = – · – –

q = – – · –

ö = – – – ·

Tables 3-7 also serve to aid in memorizing Morse letters. But if you really want to fix a Morse letter, its rhythm must become a part of you.

a = d e d a a

b = d a a d e d e d e

c = d a a d e d a a d e etc.

Two Morse letters are termed symmetrical with respect to one another if one arises from the other by reversing the order. A Morse letter is called symmetrical within itself if reversible. In table 3 pairs of symmetrical Morse letters are listed.

Two Morse letters are termed dual if one arises from the other by replacing dots by dashes and dashes by dots, see table 4. In table 5 (figure of a cross) the Morse letters are arranged as follows:

In the left half stand those letters beginning with a dot, in the right half stand those beginning with a dash.

In the upper half are those ending in a dot, in the lower half those ending in a dash.

From one Morse letter a cycle may be generated by cyclic substitution of the elements. One writes a Morse letter, then the one arising when the last element is transposed to the beginning, etc.

Those Morse letters which consist of only one type of element form a cycle of their own. Table 6 shows the cycles of Morse letters.

The Morse reading table /Ablesetafel/ (Table 7) serves for taking down Morse messages. When sending is slow it can be used without previous memorizing of the letters. It is intended chiefly to facilitate learning the letters.

The reader follows the letters given as dot or dash starting at the top center. If the first element is a dot, he reads off the left half, if a dash off the right half. If a dot follows, he follows the dotted line, if a dash follows he takes the solid line. When the letter is completed he reads the letter which he has reached.

In table 8 are Morse symbols for numbers, in table 9 those for foreign letters, punctuation, and procedure. Table 10 gives the American, table 11 the Japanese, and table 12 the Russian symbols used for domestic traffic.

It is important for anyone who has much to do with telegrams to learn to recognize the possible garbles.

C. Investigation of Possible Errors.

In the telegraphic transmission of a text there are in general three different types of errors. Almost always they result from imperfect work of the telegrapher:

a) A dot is confused with a dash or vice versa, thus

a . _ with . . i

e . with _ t

i . . with . _ a

n _ . with . _ a

t _ with . e

b) Omission of a dot or a dash:

h . . . . with . . s with . . i

m _ _ with _ _ _ o

In practice confusion of i and s, s and h occurs often.

c) Bad spacing:

mm _ _ _ _ and _ _ _ _ ch,

ot _ _ _ _ and _ _ _ _ _ ch,

to _ _ _ _ and _ _ _ _ ch.

Individual letters may be garbled thus as follows:

a ._ and e t . _

b _... and t s _ ...

n i _. ..

d e _.. .

c _ . _ . and n n _ . _ .

t r _ . _ .

ten _ . _.

ke _._ . etc.

To correct these errors one must keep the Morse alphabet in mind.

D. Life of Morse.

Samuel Finley Breese Morse was born 27 April 1791 as eldest son of the Reverend Jedediah Morse, known for his Geography of America, in Charlestown, Massachusetts. He studied for a time, then devoted himself to painting. He made several trips to Europe for study. On board the sailing vessel "Sully" which left Le Havre on 1 October 1832 for America he met Dr. Charles Jackson, Professor at Harvard College, who gave him the inspiration for his later ideas. Back in America he went on painting, in 1835 he was appointed Professor of the Literature of the Pictorial Arts at the National Academy. In the same year he displayed at New York University the model of a telegraph instrument which, however, received no further attention. In 1837 he came before the public with his first printing telegraph. After years of stern privation, during which he pursued his goal untiringly, Congress made him a grant in 1843. He was given $30,000 for an experimental line between Washington and Baltimore. In 1844 the first telegram was sent over this line. In the course of years Morse received many honors. He died in 1872.

The so-called Morse alphabet has undergone many changes since it was set up in 1840; although it bears Morse's name since it came into use in connection with his apparatus, Morse was not the actual inventor, instead Dr. Swaim of

Philadelphia claimed at a session of the French Academie in 1865 the formation of an alphabet of dots and dashes as his invention, basing his claim on a work published in 1829. The form of the alphabet used by the Englishman Bain with the apparatus he patented in 1843 was a modification of this, and this was in turn adopted by Morse, with unimportant modifications, and has later undergone some further minor changes to reach its present form.

****

Table 1

a	·–	k	–·–	u	··–
b	–···	l	·–··	v	···–
c	–·–·	m	––	w	·––
d	–··	n	–·	x	–··–
e	·	o	–––	y	–·––
f	··–·	p	·––·	z	––··
g	––·	q	––·–	* ä	·–·–
h	····	r	·–·	* ö	––––·
i	··	s	···	* ü	··––
j	·–––	t	–	* ch	––––

* Only in German domestic traffic, otherwise as separate letters, ae, oe, ue, and ch.

Table 2

Mnemonic words for Morse letters

a	. _	Abzug	o	_ _ _	Oberring
b	_ . . .	Biwaksalarm	p	. _ _ .	Paroleplatz
c	_ . _ .	Cigarrenband	q	_ _ . _	Quittungskarte
d	_ . .	Dienstkraftrad	r	. _ .	Rasenplatz
e	.		s	. . .	Stadtbahnfahrt
f	. . _ .	Fahrradlehrbahn	t	_	Tod
g	_ _ .	Gewehrschaft	u	. . _	
h	. . . .	Handapparat	v	. . . _	Vacha, Sachsen
i	. .		w	. _ _	Wachtmeister
j	. _ _ _	Jahreswende	x	_ . . _	X-Angabe
k	_ . _	Kommando	y	_ . _ _	Ystadt Schweden
l	. _ . .	Landwehrmannschaft	z	_ _ . .	Zimmermannsaxt
m	_ _	Mundblech	ch	_ _ _ _	Christbescherung
n	_ .	Nordrand			

Table 3

Pairs of symmetrical letters				Letters symmetrical within themselves			
a	. _	n	_ .	e	.	t	_
b	_ . . .	v	. . . _	h	. . . .	x	_ . . _
c	_ . _ .	ä	. _ . _	i	. .	ch	_ _ _ _
d	_ . .	u	. . _	k	_ . _		
f	. . _ .	l	. _ . .	m	_ _		
g	_ _ .	w	. _ _	o	_ _ _		
j	. _ _ _	ö	_ _ _ .	p	. _ _ .		
q	_ _ . _	y	_ . _ _	r	. _ .		
z	_ _ . .	ü	. . _ _	s	. . .		

Table 4

Pairs of Dual Letters

a	. _	_ .	n
b	_ . . .	. _ _ _	j
c	_ . _ .	. _ . _	ä
d	_ . .	. _ _	w
e	.	_	t
f	. . _ .	_ _ . _	q
g	_ _ .	. . _	u
h	. . . .	_ _ _ _	ch
i	. .	_ _	m
k	_ . _	. _ .	r
l	. _ . .	_ . _ _	y
o	_ _ _	. / . .	s
p	. _ _ .	_ . . _	x
v	. . . _	_ _ _ .	ö
z	_ _ . .	. . _ _	ü

Table 5

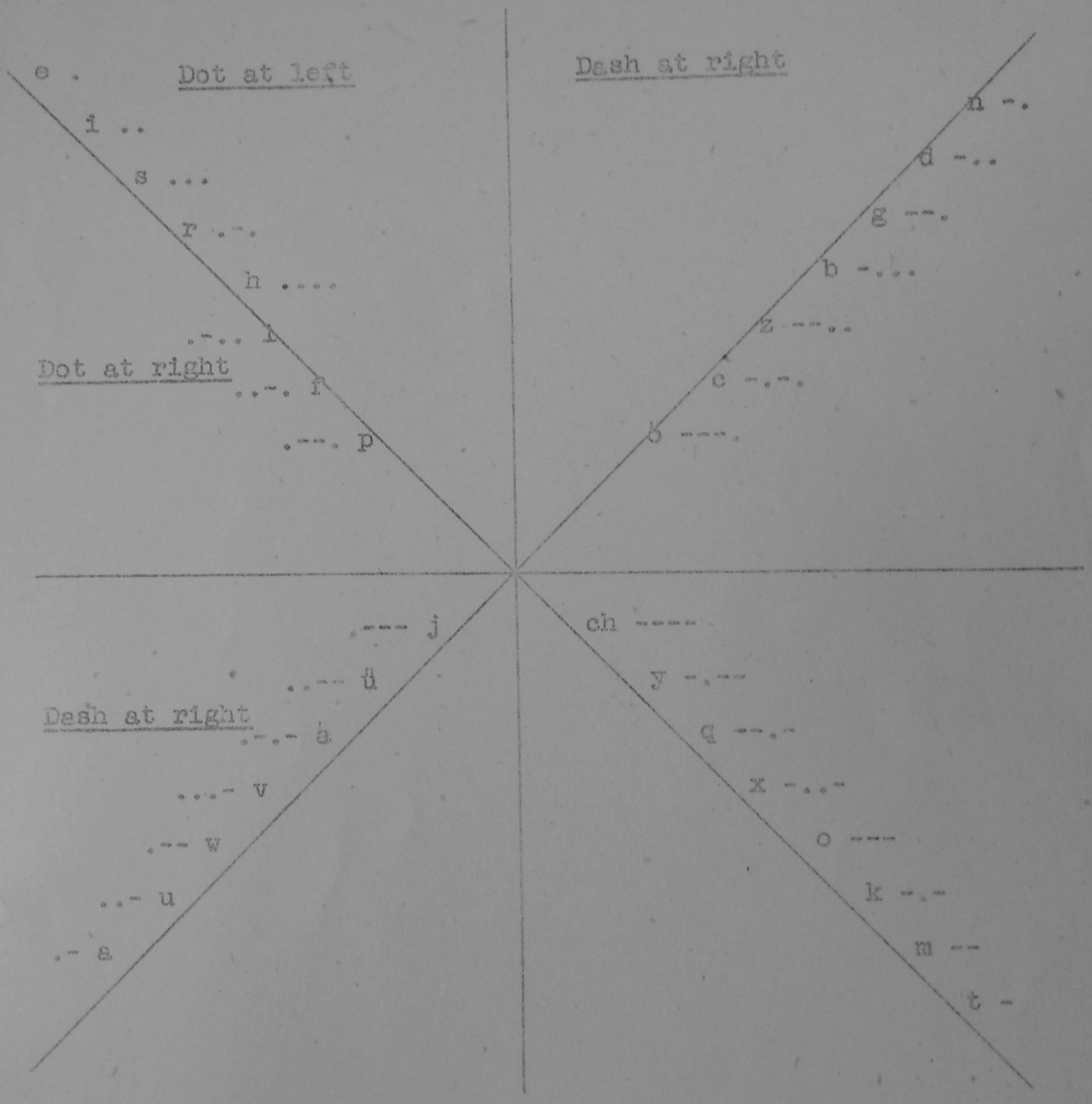
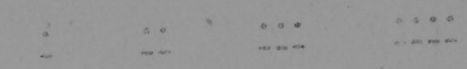

e .
Dot at left
i ..
s ...
r .-.
h ....
.-.. l
Dot at right
..-. f
.--. p
Dash at right
n -.
d -..
g --.
b -...
z --..
c -.-.
ó ---.
.--- j
..-- ü
.-.- ä
...- v
.-- w
..- u
.- a
ch ----
y -.--
q --.-
x -..-
o ---
k -.-
m --
t -

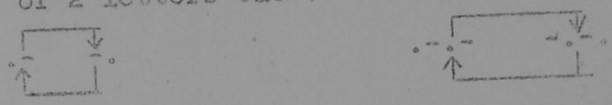
Table 6

Cycles of Morse Letters

1. Of the following 8 letters each forms a cycle of its own consisting only of dots or dashes:

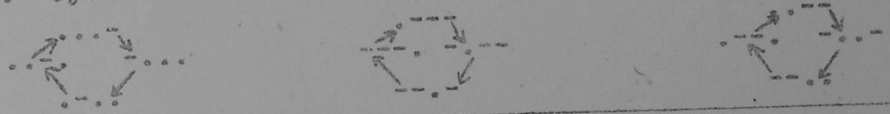


2. Cycles of 2 letters each:



3. Cycles of 3 letters each:

4. Cycles of 4 letters each:



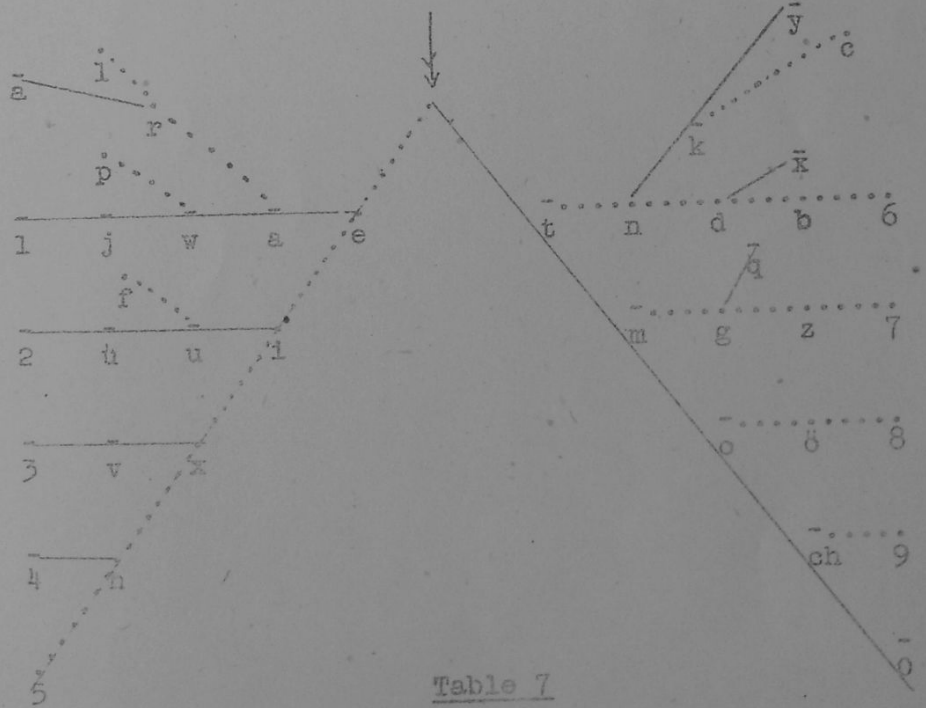


Table 7

Table 8

	Numerals		Abbreviated Numerals	
1	. _ _ _ _	1	. _	= a
2	. . _ _ _	2	. . _	u
3	. . . _ _	3	. . . _	v
4	. . . . _	4	. . . . _	
5	. . . . .	5	. . *	e
6	_	6	_	
7	_ _ . . .	7	_ . .	b
8	_ _ _ . .	8	_ . .	d
9	_ _ _ _ .	9	_ .	n
0	_ _ _ _ _	0	_	t

*or . . . . .

Table 9

á or å	.--.-	Question mark (?)	..--..
é	..-..	Apostrophe (')	.----.
n̄	--.--	Dash (-)	-....-
∝	..-..	Diagonal (/)	-..-.
β	-...-	Parenthesis ( )	-.--.-
ɣ	-.-.-	Open and close quote (" ")	.-..-.
δ	.-.-.	Underscore (before and after passage to be underscored)	..--.-
ε	--.--		
ϰ	.--.-	Message beginning	-.-.-
π	--.--	Equality sign (=)	-...-
Period (.)	.-.-.-	Separator between whole number and fraction or between letters and numbers in mixed test	.-..-
Semicolon (;)	-.-.-.	Example:	
Comma (,)	--..--	25 a 1 = 25 .-..- a .-..- 1	
Colon (:)	---...		

Table 9 (Cont.)

I understand	...-.
Error	.....
Cross	.-.-.
Start sending!	-.-
Wait!	.-...
End of traffic period	...-.-

Table 10

American Morse (Domestic Traffic)

		Frequent errors:	Numerals:		Frequent errors:
A	.-	i,f,et	1	.---.	p
B	-...	d,h,ts			
C	.. .	s,z,ic	2	..-..	3
D	-..	b,ti			
E	.	t	3	...-.	4
F	.-.	r,q,en			
G	--.	n,c,me	4	....-	3
H	....	ş,p,z,y,es			
I	..	s,i,e	5	---	
J	-.-.	c,k,ke			
K	-.-	j,n,ta	6	.....	p
L	⊢⊣	t,n			
M	⊢⊢	n,a,tt	7	--..	
N	-.	o,t,te			
O	..	n,i,ee	8	-....	
P	.....	h,s			
Q	..-.	f,g,u,in	9	-..-	x
R	. ..	s,i,ei			
S	...	h,r,i	0	⊢⊣⊢⊣	1
T	-	l,e,n			
U	..-	v,a,w,it	Period	.-.-..	
V	...-	u,st			
W	.--	f,a,u,m,at	Comma	.-.-	
X	.-..	l,y,f,ai			
Y	.. ..	h,n			
Z	... .	h,c,se			
&	. ...				

Table 11

Japanese Syllabic (Domestic) Traffic

	a	i	u	e	o
	a --.--	i .-	u ..-	e -.---	o .-...
k	ka .-..	ki -.-..	ku ...-	ke -.--	ko ----
s	sa -.-.-	shi --.-.	su ---.-	se .---.	so ---.
t	ta -.	chi ..-.	tsu .--.	te .-.--	to ..-..
n	na .-.	ni -.-.	nu	ne --.-	no ..--
h	ha -...	hi --..-	fu --..	he .	ho -..
m	ma -..-	mi ..-.-	mu -	me -...-	mo -..-.
y	ya .--		yu -..--		yo --
r	ra ...	ri --.	ru -.--.	re ---	ro .-.-
w	wa -.-	(w)i .-..-		w(e) .--..	wo .---

n = .-.-.

Soft sign .. Example: .-.. = ka, .-.. .. = ga

Hard sign ..--. Example: -... = ha, -... ..--. = pa

Separator (comma, dash, quote) .. .. ..

Table 12

Russian Morse (Domestic Traffic)

а	.-	к	-.-	ф	..-.
б	-...	л	.-..	х	....
в	.--	м	--	ц	-.-.
г	--.	н	-.	ч	---.
д	-..	о	---	ш	----
е	.	п	.--.	щ	--.-
ж	...-	р	.-.	ъ	-.--
з	--..	с	...	ь	-..-
и	..	т	-	ю	..--
й	.---	у	..-	я	.-.-

Translated by Dr. Ray W. Pettengill
6 August 1945

TOP SECRET

TIXX/46

Amt.Ausl./Abw....

Abw...../II Stahndorf, 5.12.40.

To

Foreign Office

Att.Reg.Rat.HOFFMANN

In the inclosed document is sent an introduction to the use of ciphe machine and the placement positions of the following offices abroad:

1.	Adolf: Anton Karl	4th and 5th group
2.	Benito: Anton Emil	1st and 5th group
3.	Bernhard, Emil	4th and 8th group
4.	Berta: Fritz	2nd and 11th group
5.	Ida: Anton Dora	2nd and 6th group

The first four letters of the above groups form the message key, while the fifth letter is a null and is not to be enciphered.

1. Inclosure

Instructions for Keys

Basic information concerning keys:

For enciphering with the cipher machine, there are, of necessity a) daily keys, and b) message keys.

a) The daily key changes daily at 0000 hours and is a special one determined by schedule. It consists of an internal and external setting.

To the internalsetting belong wheel arrangement and Ringstellung. The wheel arrangement is the order in which the separate wheels are placed in the cipher machine from left to right. The left wheel remains fixed, so that three wheels can be changed.

The ringstellung is the placement of the letter-ring (tire) on the cipher wheel.

Example: The Internal setting

Wheel arrangement			Ringstellung
I	III	II	F L B W

means that the cipher wheels I, III, II are to be placed from left to right on the wheel shaft and that the clip is to be locked into the hole of the tire (at the following places):

the umkehrwals	next to the letter F
wheel I	next to the letter L
wheel III	next to the letter B
wheel II	next to the letter W

TOP SECRET

The external setting is that setting visible in the four windows of the cipher machine from left to right, and is designated in the schedule as the basic setting (Grundstellung). It is used only for the formation of the indicator group.

Example: External setting (Grundstellung) MIWF means that the four cipher wheels have each been turned to such a point that, from left to right, the letters MIWF appear in the four windows.

b) The message key is a four letter group which is to be set, from left to right, in the windows, wherewith the encipherment and decipherment of the text of the message begins. The message key is chosen by the encipherer at random and is transmitted to the reciever enciphered in the indicator groups. For deciphering, it must be removed from the indicator groups. For each telegram, a different message key must be chosen.

Indicator groups: Each enciphered message contains two indicator groups, in which the enciphered message key is contained. The indicator groups proper are four letters long, the fifth letter of the group concerned (in which the indicator group is found) is a null and will not be typed out. From the typint out of both indicator groups, the daily key will be given twice. Naturally, the two indicator groups must not be enciphered again with the text proper.

Enciphering: Set the daily keys. Choose and type out the message key. Form the indicator groups and insert them into their proper places in the message. Using the message key as the basic setting, type out the text of the message and enter the letters which light up as five-letter groups.

Deciphering: Set the daily keys. Strike out the last letters of the indicator groups, and type out the indicator groups. Set up the resulting message key. Type out the five-letter message groups and read the clear text from the letters which light up.

Trans. by Lt. M.C.Lane,
Aug. 1945

Form R.1.—February, 1932.
(Revised, November, 1939).

MINUTE SHEET.

CX .. /1862.....

Source .....

No. 14

Date .....

DISTRIBUTION

V.G.

Ref. Dudley-Smith's letter DS/1019/1419 27.8.45 on Harold KIRFEL.

K.'s W.R. case officer has been asked to ensure that KIRFEL is given an opportunity of saying what he knows of Japanese Codes and Cyphers, though I think he was probably more of a language than a cypher expert.

I enclose a copy of the paragraph dealing with Japanese Secret Communications from the Tactical Interrogation report JZX 1860 (OSS SCI Rome) 2nd August 1945, and will of course let you know the results of his 020 interrogation.

Will you let us have any further questions for KIRFEL, unless you prefer to wait until you have seen his 020 report?

V.F.10 DR
18.9.45.

ACTION PROPOSED

Copy

C. Japanese Secret Communications.

6. In November 1944, Subject's section of Abt VI obtained the Manchurian code through agent Alla MEYER, chief secretary of the Manchurian Embassy who took the code out of the Embassy safe and put it back after it had been photographed. One photostat was kept with Amt VI and another was handed over to OKW-Chi (Chiffrierabteilung), directed by the mathematician Dr. HUETTENHEIM. The Japanese expert of OKW-Chi was first Lt. Dr. ADLER (about 32 years old, 1.70 m, oval face, youthful intelligent expression, possibly to be located through Assessor TROMEL, secretary of the German-Japanese Society, Berlin, Ahernstrasse 1 or 2).

7. The Code consisted of abook about 300 pages with an introduction in Japanese and divided into an encoding and decoding section. It conta ned numbers of 4 digits from 0000 to 9999 (or 8888), and to each number corresponds a Japanese sign standing either for a word or for a grammatical form of a noun, verb, etc. As the coded messages of the Manchurian Embassy consisted of groups of 5 numbers, however, some additional operation was necessarily involved after the encoding had been done according to the book and Dr. ADLER was unable to find the solution to t is problem.

8. While messages of the Manchurian Embassy were sent in groups of 5 figures, those of the Japanese Embassy consisted of groups of 5 letters. Subject believes, however, that the two systems were not entirely independent from each other and that the Japanese system too was ultimately based on the code stolen from the Manchurian Embassy.

9. Code-clerk in the Manchurian Embassy was a Japanese called KASAI. He should be fully informed about all technicalities connected with encoding and decoding.

10. A cypher machine was kept in the private apartment of the Manchurian Embassy councillor EHARA. According to subject, the Japanese cypher machine is fundamentally different from all other cypher machines in use.

11. Messages from Berlin to Tokyo went via Harbin, messages from Tokyo to Berlin via Madrid.

TOP SECRET

HS/15(g)/1488

13

Major Mason, Section V.

(Through Section V G).

Reference CX 1862 of 30/8/45. The following are the questions we should like put to KIRFEL. The paragraph references are to the interrogation report JIC 1860.

(1) What success did German cryptanalysts have with Japanese systems

Para 6 :-

(2) What other Japanese crypto materials were lifted ?

(3) Was all cryptographic material lifted by Ant VI passed to OKW/Chd. and was any other cryptographic organisation provided by Ant VI with such material ?

Para 8 :-

(4) What reason has KIRFEL for thinking that Japanese and Manchurian cipher systems were not independent ?

(5) Why should he think the Japanese system was based on the Manchurian ?

(6) When he speaks of the 'messages of the Japanese Embassy', does he seriously suppose all messages to have been in the same system ? How did he obtain access to Japanese cipher messages emanating from Berlin ? (By intercepts, photographs of telegrams, etc. ?). What amount did he see ? What would be his estimate of the bulk of cipher traffic sent by the Japanese in Berlin per day (or month or year) ?

Para 10 :-

(7) Describe fully the Japanese machine mentioned. Could Germans read the machine messages ?

Please turn over

(8) With what other cipher machines is he acquainted ?

(9) Was this machine used, or just stored in HIARA's apartment ?

28th September, 1945.

Copy to :-

Mr. F.A. Kendrick.
Major J. Seaman.
Ticon Duty Officer.

TOP SECRET U.

To: Commander Dudley Smith, Station X.

From: Mr. F.A. Kendrick, Berkeley Street.

Date: 26th September, 1945.

Interrogation of KIRFEL.

I append Thornett's suggestions. K. might also be asked if all cryptographic material lifted by Amt VI was passed to OKW/Chi and ~~whether~~ any other cryptographic organization was provided by Amt VI with such material.

Judged from his recorded statements he does not seem likely to be a very fruitful or reliable source of cryptographic information.

F. A. Kendrick

TOP SECRET 'U'

Para.8:—

(4) What reason has Kirfel for thinking that Japanese and Manchurian cipher systems were not independent?

(5) Why should he think the Japanese system was based on the Manchurian?

(6) When he speaks of the 'messages of the Japanese Embassy', does he seriously suppose all messages to have been in the same system? How did he obtain access to Japanese cipher messages emanating from Berlin? (By intercepts, photographs of telegrams, etc?) What amount did he see? What would be his estimate of the bulk of cipher traffic sent by the Japanese in Berlin per day (or month, or year)?

Para.10:—

(7) With what other cipher machines is he acquainted?

(8) Was this machine used, or just stored in EHARA'S apartment?

Japanese Diplomatic Section
24/ix/45

TOP SECRET

DS/15(Q)/1464

Mr. F.A. Kendrick

With reference to the attached documents, I would be grateful if Thornett, or anyone else concerned, could provide me with a questionnaire for KIRFEL.

Major Seaman has suggested the following questions :-

(1) What other Japanese crypto materials were lifted ?

(2) What success did German cryptanalysts have with Jap systems ?

(3) Describe fully the Japanese machine mentioned para 10. Could Germans read the machine messages ?

Would you please return the enclosures in due course with your reply.

R. Shackerlane.
for Cdr. Dudley-Smith.

18th September, 1945.

Captain Thornett

What do you suggest ?

F. A. K. 23/IX/45

Form R.1.—February, 1932.
(Revised, November, 1939).

MINUTE SHEET.

CX. 11862
Source
No.
Date

DISTRIBUTION

V.G. 3/8
for
Cmdr. Dudley-Smith

With reference to your letter DS/1019/1419 of 27th August, the attached report on Dr. KIRFEL may be of interest to you, if you have not already seen it.

KIRFEL is now at Camp 020 and War Room have been instructed to have him interrogated on the question of Japanese codes and cyphers. However, as the interrogators have not been briefed on this subject, it would help a great deal if you could let me have some more specific questions to put to KIRFEL.

V.F.7.
30.8.45.

ACTION PROPOSED

178 F

: COPIED IN WAR WOOM :
: DATE: 23-8-45 :

T O P S E C R E T

NO ACTION TO BE TAKEN ON THIS COPY.

45?

Mem: JZX-1860

2 August 1934.

To : SAINT, Washington

From : SAINT, Rome (BB008)

Subject : Tactical Interrogation of Dr. Harald KIRFEL

Reference : Our JZX-1647, dated 8 July 1945.

1. As a result of London's action on para 2 of our JZX-1647, this Unit was granted AFHQ permission to conduct a tactical interrogation of Subject.

2. In addition to clarification of questions arising in Plan CAESAR, Subject gave the following information on the JIS and on other personalities who should be priority targets for SCI Units in Germany and Austria.

TACTICAL INTERROGATION OF DR. HARALD KIRFEL

A. The Working of the Japanese IS in Germany:

3. The Japanese IS operated extensively in Germany through social and commercial contacts and conversations of the Japanese living in Germany and used many Germans as information channels without their direct knowledge. There definitely existed, however, also the paid agent type. The Axis situation favored the emergence of an intermediate type of agent who accepts gifts but is not on a regular payroll, as gifts were much more valuable in Germany than money and also because providing information for the Japanese ally was not considered treasonable.

4. Subject states that there were about 3,000 agents of the JIS operating in Germany. This included a great number of foreigners, such as Chinese seamen, White Russians, Poles, Indians, Czechs, etc. Among Germans, Subject has a specific suspicion against one German, Dr. Hermann LUFT, who maintained friendly relations with such Japanese as Dr. SATO and UCHIDA. Other possible Japanese agents known to Subject are:

a) Dr. OUCHIN, a White Russian girl who worked in the Manchurian Embassy. She might be also a Russian agent.

b) Miss ARENS, mistress of Gen.KONATZU ? KOMATSU and secretary in the Heereswaffenamt.

The Poles are said to have had important connections with the JIS. Subject states that NAKAGAWA, secretary of the Manchurian Embassy, played a "certain" role in the genesis of the WARSAW uprising of 1944.

B.....

B. Additional data on certain Japanese Personalities:

5. a) Dr. SATO:- Ministry Counsel, representative of the Japanese Ministry of the Interior in the Japanese Embassy, pro-Russian. Representative also of the Japanese Secret Field Police "KEMPEI" and one of his main tasks consisted in learning everything possible about German Gestapo methods. He was in direct contact with the Secret Service of the War Ministry.
Secretaries: YOTSUMOTO and Miss KRUG (living in BERLIN-ZEPERNICK).
Being pro-Russian, he decided to wait for the Russians with other Japanese civilians in BERLIN-BELITZ.
Inner circle of SATO: Dr. MIYASAWA- dangerous individual, general helper for SATO. Dr. HARA- Asahi Shimbun representative. Dr. KATO - Nichi Nichi Shimbun representative.

b) MAYEDA - Studied in HEIDELBERG, is very educated. Pro-American. Member of the cultural relations section of the Embassy. Not believed to have had more than normal contacts with the Secret Service. Was lecturer of Japanese at VIENNA University 1944-45.

c) MOTONO - Anti-Russian, pro-Western democracies, anti-OSHIMA. Very rich and educated. His wife is half-French. A friend of LAVAL and well informed about the conversations between HITLER and LAVAL.

d) KITAHARA - Author of philosophical treatises. Directed an East Asia Institute in VIENNA and was in contact with the JIS for purposes of economic and technical espionage as well as an observer of political and intellectual currents in Germany. Is ultra-nationalist, hostile to practically every foreign country. Professor DONAT, teacher of Japanese at the Berlin University, knows him well.

e) SUMA - Japanese Ambassador in SPAIN - Chief of the Japanese Secret Service for Western Europe. Pro-Allied.

f) ONODERA - Japanese military attache in STOCKHOLM, pro-Russian, if not actually controlled by the Russians. Source of numerous items of information hostile to Germany.

C. Japanese Secret Communications.

6. In November 1944, Subject's section of Amt VI obtained the Manchurian code through agent Alla MEYER, chief secretary of the Manchurian Embassy who took the code out of the Embassy safe and put it back after it had been photographed. One photostat was kept with Amt VI and another was handed over to OKW-Chi (Chiffrierabteilung), directed

by the.....

by the mathematician Dr. HUETTENHEIM. The Japanese expert of OKW-Chi was 1st Lt. Dr. ADLER (about 32 years old, 1.70 m, oval face, youthful, intelligent expression, possibly to be located through Assessor TROEMEL, secretary of the German-Japanese Society, BERLIN, Ahornstrasse 1 or 2).

7. The code consisted of a book of about 300 pages with an introduction in Japanese and divided into an encoding and decoding section. It contained numbers of 4 digits from 0000 to 9999 (or 8888), and to each number corresponds a Japanese sign standing either for a word or for a grammatical form of a noun, verb, etc. As the coded messages of the Manchurian Embassy consisted of groups of 5 numbers, however, some additional operation was necessarily involved after the encoding had been done according to the book and Dr. ADLER was unable to find the solution to this problem.

8. While the messages of the Manchurian Embassy were sent in groups of 5 figures, those of the Japanese Embassy consisted of groups of 5 letters. Subject believes, however, that the two systems were not entirely independent from each other and that the Japanese system too was ultimately based on the code stolen from the Manchurian Embassy.

9. Code-clerk in the Manchurian Embassy was a Japanese called KASAI. He should be fully informed about all technicalities connected with encoding and decoding.

10. A cipher machine was kept in the private apartment of the Manchurian Embassy councillor EHARA. According to Subject, the Japanese cipher machine is fundamentally different from all other cipher machines in use.

11. Messages from BERLIN to TOKYO went via HARBIN, messages from TOKYO to BERLIN via MADRID.

D. Germans with knowledge of Japanese language and affairs:

12. Teachers of Japanese at German Universities:-

a) Professor Walter DONAT, Berlin University

b) Professor SCHARSCHMIDT, Berlin University

c) Professor KRESSLER, Bonn University, Bonn Clemensstrasse. Teacher of Subject.

d) Professor CLASSEN, Heidelberg University, scarce knowledge of language, expert on Japanese economy.

e) Professor Dr. SLAVIK, University of Vienna.

13. Colleagues of Subject at interpreter school, co-editors of military dictionary:-

a) Dr. Wolfgang HAENISCH, Berlin-Zehlendorf.

b) Dr. Frittjof SCHIELING, Berlin, Mommsenstrasse. Chemist.

14. Graduates from interpreter course:-

a) Clemens ENDRIS - Wetzlar, merchant, has been previously in Japan for the BOEHLER steel firm.

b).....

b) Wilhelm BREITKREUZ, Berlin, merchant, has been previously in Japan for the I.G. Farbenindustrie.

c) Ernst HANKOHL, architect.

d) von GLINZKY, 1st Lt. Assigned to Attache-abteilung OKW.

e) Hans KILB, Capt. Assigned to Attache-abteilung OKW.

f) Dr. von STECHOW, has knowledge of matters relating to Japanese Law, was together with Subject in charge of Far Eastern Division of the Int. Academy for Social and Administrative Sciences.

g) ARNDT, Capt., son-in-law of Generaloberst HARPE, Berlin-Wuensdorf, assigned to Attacheabteilung OKW.

h) Eduard FRISCH, engineer, Prague.

i) CLEMENT, fnu, Vienna.

j) Dr. MUELLER, Vienna or Tokyo.

k) Dr. FREUDENBERG, Muenchen-Haar.

l) KRAEMER, half-Japanese, Hamburg

m) Dr. SAEUBERLICH, Berlin

n) Ingeborg von GRONAU, daughter of the German Air Attache in Tokyo.

o) Eva KRAFT, Berlin, Kaminastrasse.

p) Dr. WALS, Berlin, assigned to the research department of the Air Ministry.

q) Dr. MIEBACH, Berlin, assigned to the research department of the Air Ministry.

r) BEUTHNER, half-Japanese, Berlin, assigned to the radio listening service of the Ministry of Foreign Affairs at the Seehaus, Berlin-Wannsee.

s) von SCHACK 1st Lt., Berlin, Attacheabteilung OKW.

t) Dr. SCHWINDT, Danzig, Technische Hochschule (Institute of Technology)

u) Major MOSSDORF, Berlin, OKW or OKL

v) HINDER, architect, Berlin, Ministry of Propaganda.

w) SCHUBERT, 1st Lt. Berlin, adjutant of the General der Flieger KESSLER who was to be the successor of GRONAU at Tokyo.

x.....

x) Dr. SCHAEFER, Berlin, Ministry of Propaganda.

15. Miscellaneous:

a) Professor Dr. HAMMITSCH and Dr. BEUEL, left during 1943 on submarine for Tokyo as interpreters for the military attache.

b). Dr. Joern LEO, Itzehoe, formerly employed in the Japanese ministry for railways, recently in Amt VI.

c) Frau Dr. WEINERT, Berlin, in Far-Eastern division of Amt VI (evaluation of information)

d) Dr. BRAUN, Legation Councillor, East Asia division chief of the Ministry of Foreign Affairs, now in SALZBURG.

e) Dr. JAKOB, secretary of Dr. BRAUN.

f) Dr. ADLER, Japanese expert in OKW-Chi (Secret Communications division)

16. Subject states that further information could be supplied by the German-Japanese Society (Berlin, Ahornstrasse 1 or 2) which was directed by Admiral FORSTER and whose secretary was Assessor TROEMEL.

17. Subject's father, Professor Dr. Willibald KIRFEL, (address: Bad Godesberg, Wiedemannstrasse 37) is a scholar of Oriental languages, Professor of Hindustani and Indology at the Bonn University, director of the Oriental Seminar. Has a thorough knowledge of the Indian circles in Germany and elsewhere and is a close friend of the Maharaja of BARODA.

E. GIS activities in the Far East:

18. Information on Far Eastern affairs reached Germany through the German Consulates and Embassies in Japan, Manchuria and Nanking, in particular through the police Attaches at these places. There also existed a secret intelligence net headed in SHANGHAI by a certain "BORIS" who sent information through the police attache of NANKING. He was in contact with a number of Germans in the Far East who appeared in his messages as sources under the cover names "FRITZ", "EMIL", "LUDWIG", "OTTO". Toward the end of 1944 it became clear that BORIS worked in contact with agents of the Russian Secret Service. He attempted to obtain authorization for conducting negotiations with the Russians for a compromise peace. Subject believes that by now BORIS is entirely under the control of the Russians. He has no details about his person except that BORIS was said to be chief of the Hitler-Jugend who had somehow remained behind in CHINA.

19. BORIS transmitted normal political, economic and military intelligence. Some of the more interesting items of information concerned are:-

a) Information about secret agreements between Japan and Russia concerning promise of non-intervention by Russia in spite of the denunciation of the Neutrality pact.

b) Information about Russian ships carrying arms and ammunition to Japanese-occupied China ports for use against CHIANG's armies. This

information.....

information came through on 2 different counts in the latter part of 1944. (Similar information - concerning Russian promise to supply Japan with tanks in case of a worsening of the Japanese military position, in exchange for a Japanese promise to hand over Manchuria, Korea and even the use of some Japanese Pacific ports to Russia - was given out in BERLIN by Dr. OGA, cultural Attache and member of the Japanese Information Service, and by KAWAHARA. KAWAHARA dismissed the denunciation of the Neutrality Pact by Russia as an insignificant gesture in view of secret agreements between Japan and Russia).

c) BORIS also reported about the progress of the negotiations between CHUNGKING and YENAN and about the friction between CHIANG KAI CHEK and Gen. STILWELL. In connection with this, KOISO gave a mission to General UGAKI to come to a compromise peace with CHUNGKING China. UGAKI infiltrated high Chinese officers of the WANG CHING WEI regime to CHUNGKING for negotiations, but the Donald NELSON mission foiled the plans of the Japanese,

d) BORIS also reported the existence of a secret association under KONOYE favoring capitulation to the Allies.

20. Information from BORIS and from other sources led to the belief at the end of 1944 that peace between Japan and Chungking China was imminent. This belief was based on the following:-

a) Rumor that Madame CHIANG KAI CHEK was going to sue for divorce. As she was considered the representative of the pro-American faction, this rumor was interpreted as the consequence of an imminent anti-American move on the part of her husband.

b) Elimination of members of the SOONG family from the Cabinet.

c) Death of WANG CHING WEI in Tokyo which made it possible to unite the NANKING and CHUNKING regimes under CHIANG. In this connection German circles had their doubts about the naturalness of WANG CHING WEI's death, in spite of his long disease.

21. Ever since the second half of 1944, the GIS was preparing for the eventuality of a betrayal by JAPAN and the possible switching over of the fronts (Russia and Japan vs the Western Powers and Germany). Consequently Ant VI prepared an informer net for the Far East which was to have three centers:

a) Cap St. Jacques.

b) Kalgan, Mongolia

c) Shanghai

Except for the selection of some personnel, this plan remained on paper.

22.....

22. In connection with the already reported document on conversation between Russian and Japanese officials in MOSCOW concerning future Russian plans (see para 31), Subject adds that it was obtained by Kommando "ROLAND", one of the special units of Amt VI.

F. G-2, 5th Army report of Subject:

23. We further reproduce without comment, the following report on Subject conducted by the G-2 Interrogation Center, 5th Army on 4 June 1945. This report is No. 118, CIT. Ref: CICF serial No 223 referred to in para 5 of our JZX-1647. The following interrogation was written by Capt. KOLISCH of 5th Army.

24. KIRFEL, Harald Dr. (Diplomat). Date and place of birth: 1914, SIEGBORG, Rhineland. Home address: SIEGBORG, Kaiserstrasse 51. Civilian occupation: Law student, German Foreign Office Liaison Officer (Administration) at GASTEIN. Party affiliation: SA since 1932. He joined the party in 1934. Does not remember his number. GIS career: In March 1940 Subject joined ABWEHR AMT III, BERLIN. Owing to his excellent knowledge of Chinese and Japanese he was assigned to the Far Eastern Section of the AUSLANDSBRIEFPRUEFUNGSSTELLE. This was a sub-section of the Censorship Department of AMT III, responsible for collating, evaluating and editing information obtained from censorship. Subject's CO was Maj. Dr. THURNAU who was later promoted to Lt. Col. and placed in charge of the censorship Department of AMT III. Subject handled all important censorship extracts from letters written by Far Eastern nationals from all over the world. These letters were channelized through the Far Eastern Section of the Censorship Department in BERLIN which passed on the relevant material to Subject.

25. In September 1940 Subject was transferred to the interpreter school in BERLIN and, after passing examinations in Japanese and Chinese, was made instructor in these languages with officer status. During this period he prepared a comprehensive Manual on the Japanese Armed Forces (including the Japanese Intelligence Services) for the use of students at the interpreter school and for German officers who were attached to the German Military Attache's Staff in Japan. The latter were also trained by Subject. Information in this Manual were obtained partly through German Secret Intelligence sources in Japan and partly from Subject's own numerous contacts with Japanese officials in BERLIN.

26. In October 1940 Subject was transferred to the Far Eastern Section of the Academy of International Social Science. Professor HOEHN was in charge of this section. His deputy was Dr. SATO, councillor to the Japanese Embassy in BERLIN. During this period, Subject contacts Maj. WEIHRAUCH of AMT VI of the RSHA and sold him the idea of setting up an anti-Japanese Offensive and Defensive Section which would come directly under AMT VI. The work of this section would have been:- (1) To obtain all possible information on the activities of Japanese nationals in GERMANY and the occupied territories; (2) to obtain political intelligence on JAPAN through contacts with Japanese diplomatic and other official representatives, and through agents in GERMANY especially selected for this kind of work; (3) to recruit and organize a network of agents and informers who would subsequently be sent to operate with radio communications in INDO-CHINA, CHINA, YUNAN and THAILAND. The department was created as a result of objective appreciation of JAPAN's long term cynical policy which aimed at complete exploitation of GERMANY, so long as this was possible, for her own immediate war aims. Subject states that as of the end of 1943 all plans made by JAPAN were based on the assumption of a German collapse.

27 .....

27. Subject continued to work at the Academy of International Social Science (Far Eastern Section) as a cover for his intelligence work and also because it provided him with useful contacts.

28. In October 1944 Subject was appointed by the German Foreign Office to be administrative Liaison Officer to foreign diplomatics (in particular representatives to Far Eastern countries) who had been evacuated to GASTEIN in AUSTRIA from BERLIN. At GASTEIN he continued his intelligence duties reported to AMT VI in BERLIN by courier. He accompanied two Japanese diplomats to MILANO immediately prior to the German collapse and surrendered there to the Allies.

29. Subject worked in collaboration with Dr. KLASSEN, Professor at HEIDELBERG University, a Japanese scholar, who had spent a great deal of time in the Far East. Working under the Subject's direction were the following volunteers (VAU-LEUTE) and paid agents:-

VAU-LEUTE

a) TRANF ANTRON)
b) VAN MUC) Indo-Chinese with contacts in the Japanese
c) VAN WANG) Embassy. They were to have formed part of a special espionage network in JAPAN which was being organized by the Subject for service in the Far East; all of them were anti-Japanese. They should still be in BERLIN.

d) LEO, Dr. A German with considerable Japanese experience.
e) HERZFELD, Frau Dr.) Both had considerable social contacts with
f) WEINERT) Japanese and other Far Eastern circles in BERLIN.

PAID AGENTS

g) MAYOR, Miss Alla. White Russian, worked in the Manchurian Embassy, mother was murdered in the Russian Revolution, her father escaped to JAPAN, but was handed back to the Russians by the Japanese. She may still be in BERLIN.

h) TOTSKY, Ilona Estonian girl who had contacts in the Japanese Embassy.

i) German girl Subject cannot remember her name. She was Chief Secretary to the Japanese Attache.

30. All the above agents had their own network of informers, details of which are unknown to Subject. Besides these, there were also some unwitting Japanese sources classified as "I-LEUTE" by Subject. Subject's section also carried out special operations on the Japanese diplomatic premises which consisted of removing, photographing and then replacing documents of military and political interest. Such operations, which of course effected a great deal of information, details of which Subject is prepared to give, were obtained through friendly "inside contacts".

31. Subject spoke of a document removed (he does not know how) from a Japanese official, and passed on to him by AMT VI. It described a meeting of JAPANESE and RUSSIAN officials in MOSCOW in January 1945 at which the Russians clarified their foreign police in respect to JAPAN and the Western POWERS. They stated that their immediate aim was to occupy as much of GERMANY as possible, including, in particular,

the.....

the industrial areas of MAGDEBURG, DESSAU, KASSEL and all the RUHR province. They would then exploit German technical experience to build up the present deficiencies in their own armed forces, particular precision instruments, instruments for use in their Air Force, etc. Only then would RUSSIA be in a position to declare war on the Western Democracies and assist JAPAN in the Far East. This document was, according to Subject, dated February 1945. CHANDRA

32. Subject stated that HAMBIER, GHANDI BOSE's FREE INDIA representative in GERMANY has informed him that he had been ordered by BOSE shortly prior to the collapse of GERMANY to instruct FREE INDIA soldiers fighting for Germany to surrender to RUSSIA and not to the Western Allies. HAMBIER added that arrangements had already been made for himself to surrender to the RUSSIANS as a result of secret agreement between JAPAN and RUSSIA.

Comments and Recommendations:

33. It would seem that some form of Anti-Japanese Section of the RSHA did actually exist. It is difficult, however, at this stage to gauge how far Subject has exaggerated the scope of his own activities in order to give himself a "build-up". The possibility that the relations have been invented on the basis of directives issued him prior to the collapse of GERMANY cannot be overlooked. The presentation of the facts certainly is in keeping with Nazi Propaganda Technic.

mp

Distribution:

cc: Col. Earle B. NICHOLS (1)
WASHINGTON (6)
LONDON (6)
SCI/Z/Milan (1)
SCI/Z/Genoa (1)
SCI/Z/Turin (1)
SCI Unit/A (1)
CG file (1)
Files (5)

Copy to H.C.S.G. 25/9.

15(Q)

TOP SECRET - 1 - TICOM/I-103

SECOND INTERROGATION OF REG. RAT HERMANN SCHERSCHMIDT

OF PERS. Z S AUSWÄRTIGES AMT,

ON TURKISH AND BULGARIAN SYSTEMS.

(11)

Attached is a report on an interrogation carried out by Major BUNDY at the U.S. 7th Army Interrogation Centre, on 29 August 1945, covering Turkish and Bulgarian Systems solved by Pers. Z S.

See Ticom/I-63 for previous report.

TICOM

19 Sept. 1945 No. of pages 4

DISTRIBUTION

British

D.D.3
H.C.G.
D.D. (N.S.)
D.D. (M.W.)
D.D. (A.S.)
C.C.R. (2)
Lt. Col. Leathem
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (2) (via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)
Col. Lewis Posell, USSTAF

TICOM

Chairman
S.A.C. (2)
Cdr. Bacon
Lt. Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. Cowan
Lt. Fehl
Ticom Files (4)

Additional.

Lt. Col. Thompson.

Introductory:

It had been requested that SCHERSCHMIDT should do a complete written paper on his work on Turkish and Bulgarian systems. As his eyes, after a recent operation, do not yet permit reading, the subjects were covered by interrogation instead. His memory is sketchy on many points, but it seems unlikely that a written account based on further recollection would add much substance to this account.

1. Turkish systems

a) Diplomatic.

The Auswärtiges Amt did not work on Turkish at all until 1934. S. believes that there was in fact very little Turkish traffic until after the MONTREUX Conference in that year. He had worked on Turkish in 1920 and believes that the codes remained basically the same (alphabetic, with Arabic lettering) until 1934.

1934 - early 1935. The main system in this period was a set of 3 4-digit codes used in monthly rotation. The codes were alphabetic within any one initial letter, but the order of the letters was scrambled. The codes were rarely used without encipherment by a

section, while SCHERSCHMIDT himself concentrated on book-building and translation, occasionally checking the work of the girls in case of difficulty. Book-building and translation were fairly difficult, because of the use of the Arabic lettering and because SCHERSCHMIDT himself was only learning Turkish as he went along.

The auxiliary system, used for less important traffic, had a single code, completely unalphabetic. Though theoretically more difficult, the code was used about half the time without encipherment and was built up accordingly, aided by one or two isolated cases of reencodement from the main system. The encipherment system, when used, was the same as for the main system and was solved in the same manner.

The two systems covered all the main diplomatic links. S. believed that there were other codes used for isolated links, as RIO DE JANEIRO and BUENOS AIRES, but there had never been enough material for a solution of these.

1935 - 1939. In 1935 the Turks switched abruptly to the latin system of literation and issued a new main system consisting of 3 codes used in monthly rotation as before. The old set of three Arabic-lettered codes was made fully alphabetic and was used as an auxiliary system for consular traffic.

the same solution technique was used as before. The code was at

The basic set of latin codes remained in use until 1939, when S. left the section. The codes were scrambled by sections in 1938, but the thread was quickly regained.

1939 - 1944 S.'s knowledge of the period is vague as he handed the section over to BENZING in 1939. When he wished to return to Turkish in 1943 there was difficulty (though not with BENZING himself) over his status, and he left Pers Z S entirely for a year. S. finally resumed Turkish in 1944, being almost entirely occupied in translation in the last months of the war.

He believes the basic codes became entirely alphabetic in 1939. They were always enciphered, but he does not know the exact system, nor the exact details of solution methods. It is assumed that the basic technique remained the same, and that the stripping was done by the less skilled personnel, while BENZING and one or two others did the harder jobs of book-building and translation. Almost complete success continued.

In addition to the main system S. recalls an unalphabetic Latin-literation code used from SWITZERLAND; this he believes to be an older code which had been compromised. Still another code was used from AFGHANISTAN and beginning in 1944 from GREECE. At first this was not enciphered and the book was built up to enable solution of later enciphered AFGHANISTAN traffic.

2. Turkish systems

b) Military.

While the Auswärtiges Amt did not handle military traffic habitually, the Turkish military traffic was made available to them, and they tackled it when time permitted.

The first solutions were achieved in 1936-7 and continued until 1939, although there was very little traffic in this period. The code was 5 Z, and was sometimes enciphered by a primitive method taking only one or two digits of each group and leaving the rest unchanged. Solution was aided by a common "General Staff" address which came to four groups in the new Latin literation, and by one case of a direct reencodement from a message sent in the diplomatic code.

After 1939 a new code was introduced, and S. is unable to give any details of BENZING's work on it. He has the impression that spasmodic success was achieved, but the bulk of the work on this was done by OKW. (The OKW section was headed by REG. RAT Dr. LOCKER, and had more people than PERS. Z S. S. had a low opinion of the linguistic ability of the OKW translators, and did not think the results were in proportion to the numerical difference. He believes OKW had considerable success with Turkish military systems.)

3. Bulgarian Systems. S. stressed that this was not his main job and was done largely on a spare-time basis. Before 1938 Bulgarian work was not considered important at all, and only a few

scattered efforts were made. S. went to work on it in earnest only in the Summer of 1941.

The main system consisted of two basic codes, used on the same links for material of different security importance. The codes were 5 Z, with about 20- 30,000 actual values before 1939, and 30- 40,000 thereafter. The basic code was changed once between 1939 and 1944, S. thinks in 1941, and the former top security code then became the auxiliary system.

Except for one 2-3 month period the codes were not enciphered. Up to 20 links were served by providing a different pagination for the code twice a month on a single link. Within the pages the values were written in a cyclic alphabetical order, but the cycle might start in the middle of a page and run backwards or down and then up, or in a variety of ways.

Solution depended entirely on the amount of traffic. Any major link could be solved at will if the effort could be made, and in fact from 1943 on all major links were read. The basic code had been completely recovered by that time and the pagination could be built up correctly, with the aid of "Reference", numbers, special names, and lettered values which gave very common groups. The chief difficulty was to break the additional special pages provided for the use of each link, with personal and geographical names. As a whole solution was never a difficult technical operation.

S. knows nothing of Bulgarian military systems.

(10)

TOP SECRET

DS/15(Q)/1464

Mr. F.A. Kendrick

With reference to the attached documents, I would be grateful if Thornett, or anyone else concerned, could provide me with a questionnaire for KIRFEL.

Major Seaman has suggested the following questions :-

(1) What other Japanese crypto materials were lifted ?

(2) What success did German cryptanalysts have with Jap systems ?

(3) Describe fully the Japanese machine mentioned para 10. Could Germans read the machine messages ?

Would you please return the enclosures in due course with your reply.

18th September, 1945.

Kendrick

Jo Thornett.

Suggest following further questions:

(1) What other Jap crypto materials were lifted?

(2) What success did German cryptanalysts have with Jap systems?

(3) Describe fully the Jap machine mentioned §10. Could Germans read the machine messages?

Cdr. Dudley Smith
S.A.C.

15(Q).

CX 12799/1862 returned herewith.
There is no immediate prospect of this being issued in the I series owing to pressure of work so I thought you would like to have it back in order to reply to para 2 of VFT's minute.

As regards publication in the I series do you think paras 6 – 17 inclusive would suffice?

A.V. Cowan
for TICOM D.O.

3/9/45. → Agree but wd like to film whole report because SSA requested interrogn & wd like to show them he's not primarily a crypto man. OK? DNS

From D.O.

Forwarded. I think this report (or extracts) should be issued in the I. Series.

I will have to reply to the second para of V F7's minute of 30.8.45.

Dudley Smith
Dte. 2.9.45.

PUBLIC RECORD OFFICE

Group/Class HW 40
Piece 181

TICOM/I-89 retained under S3(4) of the PRA 1958

(date) 11/2/2004
(Signed) [signature]

TOP SECRET

DS/15(9)/1435

7th September, 1945.

Dear Bull,

Herewith the brief for Fraulein HAGEN, as promised, together with spare copies of TICOM/I-22, I-27 and D-16.

I have rather spread myself on some of the items in the questionnaire, but think it better to put in too much rather than too little. Doubtless she will be unable to answer a lot of them.

In dealing with Section X (South American) you should affect an attitude of bored indifference. Don't give her the impression we're particularly interested and don't press her if she doesn't respond.

Bon voyage.

Yours sincerely,

Commander G. Bull, R.N.V.R,
Chesterfield Street.

(Copies to :- D.D.(C.S.A.)
D.D.4).

PUBLIC RECORD OFFICE

Group/Class ..... HW 40

Piece 181

Questionnaire attached to minute dated 7 Sept 1945 retained under S3(4) of the PRA 1958

(date) 11/2/2004

(Signed) .....

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

Minute dated 2 Sept 1945 reVamed under S3(4) of the PRA 1958

(date) 11/2/2004

(Signed)

copy to D.D(CSA)
31/8

15(Q)

TOP SECRET

TICOM/D-16

(6)

Attached are translations made by SSA of Annual Progress Reports by Pers. Z.S. covering 1927, 1941 and 1942 and bearing the following titles:-

1. Progress Report of the Group England and the Spanish and Portuguese speaking countries. Aug. 8, 1927.

2. Annual Report for 1941 on the Group British Empire, Thailand, Portugal, Spain, Latin-America.

3. Cryptographic Work in the Group Great Britain, Siam, Portugal, Spain and Latin America - Hagen 1-2-42

4. Annual Report for 1942 on the Section British Empire, Ireland, Thailand, Portugal, Spain, Latin America.

TICOM
28 August 1945

No. of Pages 20

Distribution

British
Director
D.D.3
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
A.D.(C.C.R.) (2)

U.S.
OP 20-G (2) (via Lt. Pendergrass)
G-2 (via Lt.Col.Hilles)
S.S.A. (2) (via Major Seaman)
Director J.I.D. USFET
(via Lt. Col. Johnson)

TICOM
Chairman
S.A.C.
Cdr. Bacon
Cdr. Mackenzie
Cdr. Tandy
Lt. Col. Johnson
Lt. Col. Lewis Powell
Lt. Cdr. Manson
Major Seaman
Major Morgan
Capt. King
Capt. Cowan
Lt. Vance
Ticom Files (2)

Additional
S.A.C. for D.D.(C.S.A.)

T O P S E C R E T

Progress Report
of the Group England and the Spanish and
Portuguese Speaking Countries

August 8, 1927

The results in this group during the last year cannot be better shown than by contrasting the messages which could then be solved with those which can now be solved. When the undersigned took over this group only Spanish messages could be read with the aid of codes then at hand. Telegrams of all other countries were then unreadable. In this respect a real change has occurred in the period concerned. Aside from Spain, in each case we had to begin at the beginning. But even for current Spanish codes new statistical studies were necessary to eliminate the many false groups. But first the encipherment of the Chilean code was worked on and solved because this offered the largest amount of material since it had been in use for two years. The reading of current Chilean telegrams and further development of the code was then taken over by Mr. Hundt to relieve the undersigned. Then the Mexican traffic was taken up as the most promising material. Most of the old keys and nearly all the current keys were solved. Along with this, preliminary work was begun on the solution of the Ecuadorian code which was then broken quite rapidly and developed. After the relationship of the Portuguese codes to one another was recognized and the basic groups interpreted and after a Portuguese speaking lady had been loaned to us for some months, the code used on the Berlin-Lisbon circuit could be worked out. Due to a change made in the early part of the year, however, work here has come to a standstill but this difficulty can be removed as soon as more material is collected.

In the beginning of 1927, after preliminary work was completed we began the solution of the Argentine code. This code is being carried forward to the point where all incoming telegrams can be solved with approximate meaning.

With the solution of the systems used by Colombia and Bolivia, work on Spanish speaking countries was in a way concluded. As for the other countries we only have material from Peru and Paraguay and in such slight quantity that it did not appear worth working on. In the last few weeks we have begun on the breaking of the British code. The work, in spite of the very scanty material, promises good results and is being continued.

One other Spanish code could be solved in the past two months. This was code "00", which naturally is not yet completely solved but the results are already promising.

Following are some details concerning codes and systems of the various countries:

Spain:

The codes available when I took over the Spanish Section continued to be used during the period under report. These codes are:

04 225 253 261 301 311

On the basis of incoming telegrams these could be further perfected and in part corrected so that now all incoming telegrams are read almost in their entirety.

Spanish codes have developed only very slowly as completely alphabetic codes. The size of the new as well as of the old code is always 10,000 groups. The oldest which are still in use are still being transposed alphabetically within the individual pages and the page numbers are transposed. In the case of the more recent codes the page numbers and the line numbers are transposed. The vocabulary of the individual pages always remains the same. Once we succeeded in determining the page numbers of a new code there were only 100 possible meanings for each group. The meaning of the individual group is therefore much easier to determine. In all Spanish codes the last two places of each group are read first. In June, 1927, a telegram was noticed in code "00" which was relayed some days later to another office in a slightly changed form in code "04". In this way it was possible to determine some 50 groups. Since then we have succeeded in determining almost all the page numbers of the code. The content of the telegrams consists chiefly of reports on shipments of weapons and on suspicious persons. Further intensive work will be required for the development of the code.

Argentina

Only one code is used for Argentine telegrams. The code is arranged alphabetically and the major part of the vocabulary is in the general section, at the close are the following special sections: spelling table, dates, numbers, year dates, list of banks, list of nations and cities as well as a list of Argentine diplomats. In spite of the systematic alphabetical structure of the code, a complete solution of the telegrams calls for a great deal of effort since the code is extremely comprehensive and offers many compound forms. The main vocabulary of the code comprises 95,500 groups to which are added the above named lists so that the total extent of the code runs over 101,000 groups. Work was begun in 1927 and the code is now so far solved that incoming telegrams can be read roughly, although not always completely.

Beginning the first of January in 1926 the number 100 was added to each 5-place group and must be subtracted before decoding.

In the traffic of the Argentine Government with the naval mission in Italy and with other naval attaches a cipher system is in use which has not yet been worked on.

Chile

Work on the Chilean telegrams which we have been able to solve since March, 1924, was started in August, 1926, and could

be completed successfully within a short time. It developed that the previously used and already solved systematic 5-letter code with 26,500 groups was still being used. Only the first and last two letters of each group were being transformed with the aid of a digraphic substitution table. The table was quickly solved and the telegrams read once more.

Ecuador

Since the end of 1923 an exchange of telegrams between the Government of Ecuador and its representative in Berlin has been observed. The telegrams consist of non-pronounceable 10-letter groups. In the autumn of 1926 we began work on this traffic and it appeared that the division of the cipher text into 10-letter groups was purely arbitrary. For encipherment a code is used consisting of 2, 3 and 4-letter groups which, after conversion, are run together and transmitted in groups of 10 letters. The division of the groups is recognized by the vowels since the first letter of every group is a vowel, while the other letters of the group are consonants. The code is not in strict alphabetical order; solution has progressed to a point where all incoming telegrams can be read entirely.

Mexico

Telegraphic traffic of the Mexican Government with its representatives abroad is entirely with the aid of cipher systems; no code is employed. When work was begun in the autumn of 1926 it came out that Mexico in the previous years used the same key for rather long periods. Not until 1926 did they begin to improve their cipher system by combining 5 alphabets of a 26-alphabet table to form a key which would be used for several days, and finally in 1927 they began to use a separate key for each telegram. The system itself consists of a 5-place Caesar, i.e., the text to be enciphered is divided into groups of 5 letters and then the first to the fifth letter of each individual group is enciphered by a particular substitution alphabet. For transmission two groups are combined, hence, incoming telegrams consist of 10-letter groups. As mentioned above, most of the back keys and nearly all the current keys have been solved.

Colombia

Colombian traffic is enciphered very much like the Mexican with the aid of 5 successive substitution alphabets. Telegrams on hand have been solved and since the tables are always used for several telegrams, solution of this traffic ought not to cause any particular difficulties in the future.

Bolivia

Like Mexico and Colombia, Bolivia for its telegraphic traffic uses a cipher system. While the two previously mentioned countries use 5 alphabets, Bolivia uses 10 in sequences. Even though the longer telegrams could be solved, the difficulty involved with this system is so great that single telegrams, particularly short ones, cannot be read.

Peru

In regard to cryptographic technique, Peru is the most advanced country of all those in Central and South America. In telegraphic traffic a 5-letter code with pronounceable groups is used which contains 10,000 to 20,000 values. Due to the extremely scanty material, 43 telegrams in 7 years, any attempt to break the system appears futile. If, in the future, more material should come in, this code should be soluble without too great difficulty, thanks to the great help afforded by the transmission of proper names by spelling system.

Uruguay

The telegraphic traffic of Uruguay is likewise so slight that no work is being done at present. Without further investigation we can say that, with more material, success could be attained without too great effort since it is merely a 2-digit encipherment employed with a short code.

Portugal

The Portuguese Government uses for telegraphic communication with its representatives 5-digit codes of 60,000 to 70,000 groups. In the autumn of 1926 we began working on Portuguese material. As formerly, so today, with Portuguese codes, the last three digits of the 5-digit code group are to be read first. It was ascertained that for each circuit a particular code existed. For the Berlin-Lisbon, Lisbon-Berlin traffic, which was attacked first, it could be shown that this code can be reduced by means of a 1000-place substitution table to a code in use earlier. The 3 last digits of the 5-digit code group, which are to be read first, correspond to the page numbers of the code which have been changed in respect to earlier codes, while the line numbers continue unchanged. When the work had progressed so far that we could recognize the approximate content of the telegrams, in February, 1927, a change took place in this traffic. Whether this new code can be reduced by any such measures to the known code has not yet been determined. On the other hand, in the case of the code used between Bucharest and Lisbon, this possibility has been proven and if more personnel is available a rapid solution should be possible.

Brazil

Since March, 1926, a new code has been used in Brazilian traffic. The work on this, begun in the past few weeks, shows that it is again an alphabetical code constructed very much like the one formerly in use. As before, the last 3 digits of the 5-digit group are read first. The number of groups, 94,800 in the old code has been expanded by 5,000 in the new code, from which we conclude that the expansion of the code has taken place by introduction of new concepts. Solution is rather difficult because of the lack of material (70 messages). However, a good skeleton has been obtained for further work in the groups already solved.

Conclusion

In conclusion it is neceasary to say a few words on the personnel question. Even though in the period under report the codes and ciphers of most of the Spanish and Portuguese speaking countries have been solved, the help available is by no means adequate to develop these codes to the point where all telegrams can be read completely. It is absolutely necessary that in the present status of the work an assistant with a complete mastery of the language concerned be available for each of the two language groups. If this is not the case, then sooner or later things will bog down again and in view of the progressive difficulty of the codes and ciphers, it will not be so easy to get a fresh start once more.

Furthermore, in the future the English materials must be worked on more intensively. The two codes worked on and solved, "B10" and "B12" call for a separate assistant to make possible further development. For the new work (numbers) one permanent assistant is the least we must have.

To make possible further successful work we should therefore need:

For English codes "B10" and "B12"	1
Statistical work	1
Spanish group	1
Portuguese group	1
Total	4

Berlin, 8 August 1927
Ernst Hoffman

Annual Report for 1941 on the Group British Empire, Thailand, Portugal, Spain, Latin America

England

Worked on:

a) English Digit Systems:
The "Interdepartmental Code". The basic code book of this system was captured and the sections of the additive sequence worked out from time to time were placed at our disposal by O.K.W. or the Air Ministry.
Some telegrams from the Middle East could be read; toward the end of the year the receipts were so light that further work on this material no longer appeared worthwhile.

b) English letter systems:
1) "B 25", a non-systematic 4-letter code with 16,224 groups. It was solved and so far developed that telegrams could be read for a considerable period almost without gap. In the autumn of 1940 a captured original was sent us which made possible complete reading of telegrams.
2) "B 22", a systematic 5-letter code with 84,000 groups. It was solved and telegrams have been read for approximately 3 years. In the summer of 1940 we were given a captured original.
3) "B 30", a non-systematic code of 4-letter groups used in the Near, Middle and Far East. Traffic received was slight; however a beginning was made in setting up an index and the cross sum of the groups as well as the size of the code was determined.

Not worked on:
The consular system and Teneriffa-Las Palmas traffic, involving transposed plain text, in which only a few telegrams were received.

South Africa

Worked on:

a) "B 22" (see England a 2), and
b) "B 23", a systematic 5-letter code of approximately the same size as "B 22" which was solved and so far worked out that the rare incoming telegrams can be read almost without gaps.

Not worked on:
A letter system used in traffic with Stockholm, due to want of material. The last telegram of this type was received 16 December, 1941.

Ireland

Worked on:

a) "B22" (see England a 2), and
b) "B22" enciphered. This involves 3-4 different Spaltenverfahren each with T26, which can be reduced to strips. The

encipherment table is so used that one 5-place group is replaced according to $T26_n$, the following group by $T26_n$ 1, $T26_n$ 2 or $T26_n$ 3 or else $T26_n$-1, $T26_n$-2 or $T26_n$-3. All Irish telegrams can be read completely.

In 1941 223 Irish telegrams were read.

Canada

Worked on:
"B 22" (See England a 2)
Not worked on:
A 5-letter system in which only isolated telegrams were received.
In 1941 583 British Empire telegrams were read.

Thailand

Worked on:
A systematic 5-digit code in English language with 110,000 groups. For the last 10,000 numerical groups usually pronounceable letter groups of indefinite length are given. A part of the telegrams is enciphered, i.e., there is added to or subtracted from the line number of the groups a multiple of 5 according to an indicator. Telegrams are read almost without gaps.
In 1941 97 Thailand telegrams were read.

Portugal

Worked on:

a) A partially systematic 5-digit code with 50,000 groups. Encipherment on the different circuits is in the following fashion:
   1. By subtraction or addition to the line number of a sum fixed for the circuit concerned.
   2. By transposition of the group elements.
   3. By 1000-place substitution tables for the page numbers.
b) A partially systematic 5-digit code with 61,500 groups. It is enciphered with 20 distinct 100-place substitution tables for the line number of the groups and on some circuits also with a 1000-place table for the pages. In addition there is a letter encipherment to avoid repititions, i.e., a 100-letter table for the line number and a 1000-letter table for the page number. Moreover, for each circuit there is a distinct transposition of the group elements.
   A large part of the telegrams were read with some gaps.
   In Berlin-Lisbon traffic telegrams sent in this code were not read because keys changed so frequently and receipts were so small that only in a few cases did the work yield any practical result.
c) A partially systematic 5-digit code with 61,800 groups with encipherments of the type described in paragraph b. The numerical encipherments were solved and beginnings made in the solution of the code. Because of the slight receipts and lack of personnel for Portuguese, work was not continued.
   In 1941 66 Portuguese telegrams were read.

Brazil

Worked on:

a) Letter systems
   1. "Bras. B1", a systematic 5-letter code with 165,625 groups. The telegrams were read almost without gap.
   2. "Bras. B2", a partly systematic 5-letter code with 82,000 groups. After 2,200 groups had been recovered and a series of telegrams read with some gaps, a copy of the original code was placed at our disposal by O.K.W. which made possible a complete reading of all telegrams.

b) Digit systems:
   1. "Bras. Z1", a systematic code with 100,000 5-digit groups. The telegrams were read almost without gap.
   2. "Bras. Z7" and "Bras. Z8". Encipherment of "Bras. Z1" by means of 1000-place tables for the page numbers and interchange of group elements. The telegrams were read almost without gaps.
   3. "Bras. Z3", a code with 80,000 digit groups, which was put together from "Bras. B2" by the exchange of the page numbers and displacement of row digits on a multiple of 10. Work has just begun (February 1942) on the still limited material.
   4. A 5-digit probably systematic code with 100,000 groups was enciphered with a table of letters. The 300 pairs of letters occurring in the first and second or fourth and fifth places were reduced by equating to a 100-place table for the first and second and one for the fourth and fifth places and the 26 middle letters (in the third place) have likewise been reduced by equating to a 10-place table. The conversion to numbers proceeded slowly because of the very sparse incoming material. From the 23rd of December 1941 to the breaking off of relations (29th of January 1942) only one telegram of this sort was received.

In the year 1941, 248 Brazilian telegrams were edited.

Spain

Worked on:

A 4-digit, partly systematic code with 10,000 groups called "04". The telegrams enciphered in this code in the traffic Madrid-Bogota, Quito, San Salvador, Sofia, San Juan de Puerto Rico and in part Guatemala were completely read. The remaining traffic was only noted. The traffic Madrid-Berlin fell off almost entirely; in 1941 eight telegrams were received.

In the year 1941, 34 Spanish telegrams were edited.

Argentina

Worked on:

a) A 5-digit systematic code with 110,000 groups. In most of the traffic there was a change of groups through addition or su subtraction of a constant sum. Occasionally, also, in one and the same telegram addition and subtraction were used interchangeably. The traffic was solved and the telegrams were read and edited almost without gaps.

Bolivia

Worked on:
A 5-digit code with 78,000 groups is enciphered with 1000 and 100-place letter code-tables for the pages and row columns and in frequently changing regrouping of the group elements. The incoming telegrams which were both very sparse and uninteresting in content could be read with some gaps.
In the year 1941 one Bolivian telegram was read.

Chile

Worked on:
A 1 to 4 letter systematic code with 42,000 groups was built up by the autumn of 1940 to such a point that the telegrams were read almost without gap. A photocopy of the captured original which was placed at our disposal at that time made possible a complete reading of the telegrams from that time on.
Not worked on:
A very sledom used systematic, 4-letter code in consular traffic (Passport) and a new diplomatic code, on account of the still limited material. Up to this time 12 telegrams have been received since the 25th of August, 1941.
In the year 1941, 273 Chilean telegrams were read.

Dominican Republic

Worked on:
Columnar system (Spaltenverfahren) with 5 T26, which is applied to the plain text. Occasionally, also, plain text passages appear in the enciphered messages - the keys were solved and the incoming telegrams were accordingly completely read. In the year 1941 one Dominican telegram was read.

Ecuador

Worked on:
A 2 to 4 letter systematic code with 61,945 groups with interspersed clear text. The code was solved and the messages could be completely read.
Not worked on:
A letter consular system, in which only one telegram was received.
In the year 1941, 25 Ecuadorian telegrams were read.

Colombia

Worked on:
Columnar systems with 5 to 15 T26, which are directly applied to the plain text without any text between. The telegrams, which came in at great intervals, were read by the solution of the current substitution table.
In 1941, 45 Colombian messages were read.

Mexico

Worked on:

a) A systematic 5-letter code with about 100 different encipherments. For this there was a device whereby each group was encoded by a group occurring in the basic code 1 to about 150 places later. The code was built up and the greater part of the encipherment solved, so that telegrams of which the key was known were completely read, and the others in part.

b) Work has now begun (February 1942) on the compilation of a new letter code book which is built on the plan outlined in (a) and is enciphered in a similar fashion.

c) Isolated consular telegrams, whose text is enciphered in columnar fashion, are in the process of being worked on.

In 1941, 47 Mexican messages were read.

Peru

Worked on:

A partly systematic 5-letter code. For the various circuits digraphic and trigraphic letter code tables were used for encipherment of the first and second letters of a group and for the third, fourth and fifth letters, respectively.

Work has begun on the solution of the code book and the substitution tables. On account of a lack of personnel the building of the code book has not been able to be continued.

Uruguay

Worked on:

A systematic 4-letter code with 2,142 groups with interspersed plain text and plain text encipherment. For this 100-place code tables were used and in such a way that for each individual letter of the plain text or for a consonant with vowel following it a 2-digit group is substituted. The code book has been worked out and the code tables currently solved, so that the few incoming messages can be completely read.

In 1941, 21 messages were read from Uruguay.

Venezuela

Worked on:

a) A 4-letter systematic code with 12,000 groups with interspersed enciphered plain text. For the encipherment of the plain text columnar methods with one to 10 T26 were used. The code book groups were changed in the various systems by a displacement of one to ten places in the code book.

b) Columnar systems with 5 to 10 T26, with which the plain text was enciphered directly without intervening text.

The solution of code book and tables has progressed to such a point that the messages can be read almost without gaps.

In 1941, 45 Venezuelan messages were read.

From Guatemela, Havana, Panama and Paraguay the incoming messages are so extraordinarily unimportant that not once was it worth taking note of them.
From Panama and Guatemala one plain text message was read.

In 1941 from this group a total of 1639 messages was read.

Personnel

Section head: Miss Hagen
Colleague on English, Portuguese and in part Spanish: Miss Wernick
Colleague on Spanish: Miss Noll
Assistants: Miss Fellbaum
" v. Kaisenberg
" Kleppin
Mrs. Offermann
Miss Roebcke
" Seele
" Titschack

Berlin: 11 November 1942

*Translated by Lt. M. C. Lane

Cryptographic Work
In the Group Great Britain, Siam, Portugal,
Spain and Latin America

Ireland

A substitution system with 26 alphabets which can be reduced to a slide is used with a systematic 5-letter code. Each 5-letter group is enciphered by one alphabet, the following group either with the next or next-but-one in the table. Sometimes the alphabets are used in reverse order with and without omissions. The tables are in use on the different circuits for several months running. Replacement dates are quite irregular.

Siam

The systematic 5-digit code is enciphered by adding to or subtracting from the 2-digit line number of the group a multiple of 5 according to an indicator (key word). Thus far no change has been made.

Portugal

a) A systematic 5-digit code is enciphered on the various circuits:

1. By adding to or subtracting from the line number a constant sum for the circuit concerned.
2. By transposition of group elements.
3. By a 1000-place substitution table for page numbers.

b) A partially systematic 5-digit code is enciphered with 20 different 100-place substitution tables for the line number of the group and on some circuits with a 1000-place table for the pages. In addition there is a letter encipherment to avoid repetitions, i.e. a 100-place letter table for the line number and a 1000-place letter table for the page number. Moreover, for each circuit there is a particular transposition of the group elements. Replacement dates are quite irregular.

Brazil

1. The systematic 5-digit code is enciphered with 1000-place tables for the pages and by interchange of group elements.
2. A seemingly systematic 5-digit code is enciphered with letter tables. The 300 pairs of letters occurring in the first and second or fourth and fifth positions have been reduced by equating to one 100-place table for the first and second and one for the fourth and fifth positions and the 26 middle letters (third position) have likewise been reduced by equating to a 10-place table. The conversion to numbers is going ahead very slowly due to the small amount of material received.

For '1.' the replacement dates are quite irregular, for '2.' no replacement has yet occurred.

Argentina

With a systematic 5-digit code of 110,000 groups on many circuits changes in the groups are made by addition or subtraction of a constant.

Bolivia

A 5-digit code of 78,000 groups is enciphered with a 1000-place or 100-place letter table for page or line numbers and by simultaneous re-grouping of the group elements. Replacement dates are quite irregular.

Dominican Republic

Substitution system with 5 alphabets applied to the plain text. Replacement quite irregular.

Colombia

Substitution system with 5 alphabets applied to the plain text. Replacement quite irregular.

Mexico

According to approximately 100 indicators each group of the systematic 5-letter code is changed into a group lying 1-100 places farther on in the decoding section. No change in mode of encipherment has been made.

Peru

As encipherment for the partially systematic 5-letter code digraphic and trigraphic tables are used for the first and second and the third, fourth and 5th letters, respectively. These tables are different for each circuit. No replacement of tables has been made.

Uruguay

Plain text interposed between groups of a 4-letter code are enciphered with a 100-place numerical table, so that for each letter of plain text or for a consonant plus following vowel a 2-digit number is substituted. Frequent endings and punctuation are represented by 3-digit numbers, e.g. 333 = ion. Replacement very irregular.

Venezuela

Plain text introduced between the groups of a systematic 4-letter code is enciphered by a substitution system with one to ten alphabets. Moreover, on some circuits the groups are pushed along from 1 to 10 positions in the code. Replacement is quite irregular.

Hagen
1-2.42

T O P S E C R E T

ANNUAL REPORT FOR 1942 ON THE SECTION BRITISH EMPIRE, IRELAND THAILAND, PORTUGAL, SPAIN LATIN AMERICA

BRITISH EMPIRE

England

Work was done on:

a) English letter systems

1. 'B 22', a 5-place systematic code*
2. 'B 25', a 4-letter non-systematic code
3. 'B 30', a 4-place non-systematic letter code constructed in the same fashion as 'B 25', but with minor variations. A change is made in the spelling procedure which in 'B 30' is but a simple substitution alphabet of 26 letters. Work on the code was begun after the construction of preliminary studies in the spring of 1942 but was again laid aside after a short time because other work was more pressing. In October, 1942, work was taken up again and by the end of the year about one thousand groups were broken. On the 21st of November, 1942, the first telegram was read. The incoming traffic was so slight and the content so uninteresting that work was not continued intensively.
4. 'B 31', a 4-place non-systematic letter code of 16,00 groups constructed in almost the same fashion as 'B25'. The code has been in use since 1 May, 1942. The preliminary work was started in May and the remaining work in June. By the end of 1942 2500 groups had been recovered. The first telegrams could be read early in October, 1942. In this code, also, traffic receipts had fallen off greatly and the content of the telegrams had decreased greatly in importance.

b) English number codes:

The 'Interdepartmental Code' (original designation). Since the traffic received was slight and in consequence the additive sequences, which were received only late from the Ministry of Aviation, revealed fragments of a text which was generally uninteresting, work was stopped in the summer of 1942.

*More detailed statements about the codes and systems mentioned in this report which were in use before February 1942 are to be found in the annual report of 1941 and the report on decipherment work dated 1 February 1942.

Not Worked on:
a) English numerical systems (except IDC)
b) A consular system used between Teneriffa and Las Palmas in which it was a case of transposed plain text. As ORR. Waechter of the F.A. (Forschungsamt) informed us in February, 1942, fruitless attempts at solution were made then.
c) The 'Indian Code' (original designation), a systematic 5-letter code which was laid aside due to lack of material after a start on solution had been achieved.
d) A non-systematic 4-letter code of approximately 17,000 groups not worked on due to lack of adequate material.

Australia

Work was done on:

'B 22' (see England a 2)

Canada

Worked on:
'B 22' (see England a 2)

South Africa

Worked on:
a) 'B 22' (see England a 2)
b) 'B 23', a systematic 5-letter code.
Not worked on:
A letter system used in traffic with Stockholm in which during the year only 7 messages were received.
In the year 1942, 546 British Empire telegrams were read.

Exchange With O.K.W., O.K.M. and F.A.

O.K.W. was given, about the end of August, 1942, Code 'B 31' (about 1500 groups) and beginning of November, Code 'B 30' (about 750 groups) for copying. Since then a regular exchange of solved groups has been carried on for 'B 31' between O.K.W. and Pers. Z.S.

O.K.M. was given on the 16th of December, 1942, Code 'B 31' (2436 groups) for copying. No exchange of groups is made.

In February, 1942, at the request of ORR. Waechter, an attempt was made to establish contact with F.A. which, however, did not get beyond a general exchange of ideas. The only concrete result was that F.A. placed at our disposal a list of approximately 50 'B 30' recovered groups.

Ireland

Worked on:
a) 'B 22' (see England a 2)
b) 'B 22' with encipherment (Spaltenverfahren).

Not worked on:
A number system due to inadequate material.
In 1942, 126 Irish telegrams were read.

Thailand

Worked on:
A 5-digit code in English language with and without encipherment. On the 7th of October, 22nd of September and 31st of December, 1942, there was a change of keys on the Berlin circuit. In place of the previously used addition or subtraction of a multiple of 5+1 to the line number of the group, a 5-place additive sequence is being used. Proper names and words not contained in the code are enciphered by a substitution table. Moreover, irregular spelling groups beginning with T used for geographical names have been replaced by others beginning with J.
In 1942, 139 Thailand telegrams were read.

Exchange with F.A.

At the beginning of 1942 the Thailand code was turned over to F.A. for copying.

Portugal

Worked on:
a) '302'*, a 5-digit, partially systematic code of 50,000 groups with encipherments. In the autumn of 1942 a new 1000-place substitution table used for this code on the Rome-Lisbon circuit was solved so that the Rome telegrams, which up to the summer of this year were mostly sent in '328' (see b) and thereafter almost exclusively in '302', could be read again.
b) '328'*, a partially systematic 5-digit code of 61,500 groups with encipherment.
c) '299'*, a partially systematic 5-digit code with 61,500 groups with encipherment.
d) Telegraphic traffic between Lisbon and Luanda in which a simple 26-letter substitution is employed for enciphering Portuguese plain text.

Not worked on, but merely watched due to inadequate material:
a) Part of the Lisbon-Berlin traffic.
b) Part of the Lisbon-Vichy traffic.
c) Traffic with Portuguese colonies with the exception of the above mentioned Luanda traffic.

In the course of the year 1942, 352 Portuguese messages were read.

Exchanged with O.K.W.

On 14th December, 1942, a photographic copy was made of the original code book '205' and of 9 of the appurtenent 24-line substitution tables which had been loaned to Pers. Z.S. by O.K.W. '205' is a basic form of the codes '299' and '328' mentioned under b) and c), and after complete solution of the remaining 15 substitution tables, which were already solved in large part, all telegrams can be read without gaps. Before the original code was turned over, a regular exchange of group meanings took place with O.K.W.

*) named for the 'e' (=and) page of the code.

Brazil

Worked on:
a) Letter systems:
1) 'Bras B1), a systematic 5-letter code with 165,000 (possible) groups.
2) 'Bras B2), a partially systematic 5-letter code with 82,000 groups.
b) Number systems:
1) 'Bras Z1', a systematic code with 100,000 groups which as yet is only used in isolated cases between Helsinki and Rio.
2) 'Bras Z3', which is derived from 'Bras B2' by shifting the line numbers and substitution of page numbers. Since material comes in very sparingly - in the course of 1942 only 54 telegrams - no telegrams could be read in spite of good progress in the work.

In 1942, 139 Brazilian telegrams were read.

Spain

Worked on:
'04' (so-called for the indicator group of the code), a 4-digit, partially systematic code with 10,000 groups.

Not worked on:
All other systems. Berlin traffic is very sparse and other circuits would have to be watched and in time worked on by a very large force. No attmept was made by O.K.W. or by F.A. In F.A. the opinion was held that machines were employed.

In 1942, 22, Spanish telegrams were read.

Argentina

Worked on:
a) Letter systems:
A 5-letter systematic code of approximately 110,000 groups
b) Number systems:
A 5-digit systematic code of 110,000 groups with additive encipherment.

Not worked on due to scant material:
A 5-letter code with approximately 110,000 groups in which during the entire year only 130 telegrams were received.

In 1942, 240 Argentinian telegrams were read.

Bolivia

Worked on:
A 5-digit code with 78,000 groups and letter encipherment. During the entire year only 6 Bolivian code telegrams were received.

In 1942, 4 Bolivian telegrams (one code, three plain text) were read.

Chile

Worked on:
Clave Solar (original designation), a 1 to 4 place, partially systematic letter code with 42,000 groups.

Not worked on:
a) A rarely received, systematic letter code for consular traffic (passport).
b) A system appearing only sporadically until mid-November, 1942. From 19th November, 1942 on, this system was introduced on almost all circuits available here. The Chilians themselves state it is a machine system, so that only very few messages sent in 'Solar' can be read. The material available apparently is not yet adequate for breaking a machine system.
In 1942, 278 Chilian telegrams were read.

Ecuador

Worked on:
A 2-4 letter system code.
Not worked on:
A consular system in letters in which only sporadic telograms were received.
In 1942, 21 Ecuadorian telegrams were read.

Colombia

Worked on:
Spaltenverfahren with 5 to 15 T26 (substitution alphabets) which lie directly above the plain text (are applied directly to the plain text).
In 1942, 69 Colombian telegrams were read.

Mexico

Worked on:
a) 'pomos'*, a systematic 5-letter code with encipherment.
b) 'xepit'*, a systematic 5-letter code very similar to 'pomos' in construction. Preliminary work was begun in February, 1942, but actual work only at the end of June. On 22nd August, 1942, the first telegram of this kind could be read. In the middle of November in France, the original code book was captured and on the 24th of November, 1942, solution of the Code was achieved before a photographic copy of the original reached us on 25 November, 1942. Since then the few telegrams received have all been in the old code book 'pomos'.
c) Spaltenverfahren with 20 T26 which lie directly over the plain text without an intermediate text (single encipherment with 20 alphabets).
In 1942, 29 Mexican telegrams were read.

Exchange with O.K.W.

On the 25th of November, 1942, photographic copy of the original code 'xepit' was delivered to Pers. Z.S. by O.K.W.

*So-called for the 'y' (= and) group.

Peru

The development of a partly solved, partially systematic letter code with encipherment has been postponed temporarily due to lack of personnel. Work will be resumed in the near future.

Uruguay

Worked on:
A systematic 4-letter code with 100 place substitution table for enciphering plain text.
In 1942, 19 Uruguayan telegrams were read.

Venezuela

Worked on:
a) A systematic 4-letter code with encipherment.
b) Spaltenverfahren with 5 to 10 T26 which apply directly to the plain text.
In 1942, 13 Venezuelan telegrams were read.

In the case of other Ibero-American States enciphered telegrams were almost entirely lacking so that only a few intercepted plain texts could be read:

Dominican Republic in the year 1942.....	1 plain text
Guatemala " " "	3 "
Havanna " " "	5 "
Nicaragua " " "	1 "
Panama " " "	1 "
Paraguay " " "	2 "

In the whole Ibero-American field the receipt of traffic fell off in consequence of breaking off of relations with Germany.

In 1942 a total of 2339 telegrams was read by this section.

Personnel Status as of 15 January, 1942

Section Head --- Miss Hagen
Subchief ------- Miss Wernick
Miss Galuschka, Phd.
SSecialist in the Spanish language: Miss Noll
Specialist in the Portuguese and English languages: Miss Ehlers
Assistants: Miss Seele (partly engaged in independent book-breaking and translation in Portuguese)
Miss Buehler
Fellbaum
Finken
v. Kaisenberg
Kleppin
Roebcke
Titschack

Hagen
1 Feb., 1943

(4)

TOP SECRET

DS/15(Q)/1414

D.D.(C.S.A.)

(Copy to :- D.D.4.)

Examination of some of the documents listed in DS/1322 of 14th July, 1945, in conjunction with the Pers ZS Annual Reports for 1941 and 1942 (DS/1262 of 14th June and 1327 of 15th July) gives the following identifications of the Pers ZS "B" classifications of British civil systems :-

(i) Certain

B.18. Foreign Office R Code (1930).

B.22. Government Telegraph Code (1933).

B.25. Foreign Office R Code (1935).

B.30. India Office Confidential Code Q (1935).

B.31. Foreign Office R Code (1941).

(ii) Probable

B.23 }
B.24. } South African versions of G.T.C.
B.26. }

25th August, 1945.

PUBLIC RECORD OFFICE

Group/Class ..... HW 40

Piece 181

TICOM/D-3 (cont'd): retained under Section 3(4) of the Public Records Act 1958

(date) 11/2/2004

(Signed) .....

Pens 25 Records (abdocts)

15(Q).

(16) B.26. Südafrika (2)

BEHUN
BYZFI
DYWXI
LOWMO
MYTKE
NAKIK
TYROW
VOZRO

✓ (9) B.17.

A.b = 1
d = 2
e-f = 3
g = 4
i-k = 5
ℓ = 6
m 7
n 8
o-p 9
q 10
s 11
t 12

$12n+1 = 13, 25, 37, 48, 61$
73, 85 usw.

AMGOL
BIDRO
DISEG
EPFAP *
FEKOM *
KASSU *
RAPTI

(Sc. M to KA)

(13) B.23

ABAIB A
ABAOD A
AJHWI all
ALUDI and
DALYI comma
GUJWH ⊙

(48) B.26. Primus Capetown
Oppenheim London } v Defence Pretoria
Saleg Berlin

(47) B.27 Primus Capetown v Saleg Berlin 4/39

? 4 Letter Book

SGHP 30/8/38 Saleg Berlin
TIYS v Primsec.
OYXV
IZZA

(? Recorded.)

(14) B.24

ANCBU and
OVEVG
UXTVI stop
YMYUW

(17) B.30

(B.25 IV (deleted).
? unused old book.

ODUD ⊙ i.e. "Q"
K2AH ⊙
WAVU ⊙

AAIG necessarily
MI 1939
PD sentenced, sentiments
QG (? statsup)
VM wise wisdom
YB have not yet, been
ABAA hundred of War Products
BH demanded.
etc.

(10) Band 1 B.18
(11) 2
(2 copies)

KYSU ⊙
SIZE ⊙
TECA ⊙

i.e. R.1930

AABY Item
CF book, letter follows
FH as the
GO Li-Tsung-jen, Liberate
HU ~~Liberate~~ and that
IX WU
ME persad, ity, of persona grata
etc.

(54) B.20 Prodrome London Bucharest

Preamble in R. 1930 (TECA)

JEBY (1932)
UDUC
FUOC
SUUN
OXYX

(48) 3.17 RAPTI (RIPTA) Prodrome Berlin
SASUK (KASSU)
OBTEI

Preamble in R. 1930

1930–32

(15) B25 ALLA ⊙ I.R. R. 1935
FAKE ⊙
NOAH ⊙

ASAD defence
BK seem
CR as most
DF sea
etc.

(56) B. 31 Prodrome in v Naples 14.3.45
(SISR)

I.E. R. 1941

NWEES PHIZK VVFQC
VQRJX VQRTW ZIONN etc.

(55) B.22 (GTC) Kraftec

AHOOA
ABLIV
A2FIV
ABABY

B. 18 ✓ R. 1930 ?

19

20 ? { ? I.D. Cipher 19--
(4-Letter groups) F.O. 4-Letter (JEBY)

21 ?

✓ 22 ✓ GTC 1933

23 Canadian/SA 5-Letter (ALUDT)

24 5-Letter (ANCBU)

✓ 25 ✓ R. 1935

26 SA 5-Letter (BEHUN)

27 ~~? I.D. Cipher 1934~~ SA. 4-Letter (TIYS 122A)

28 ?

29 ? I.W.C.

30 ✓ Q. 1935

31 ✓ R. 1941

C.O. Confid.

D.O. Confid.

? Q Later than 1935.

(I.D. Prev. 1936
5-Letter groups)
? 4-Letter groups

I.D. 1924
-1931

DS/1327 of 15 July
1322 14 July
1262 14 June

Pers. Sig. Title	Book	Description	In force	Folder of Traffic	Remarks
B.17		5-Letter (9) Few Statistics		(48) 1931/32	F.O. (KASSU)
B.18	✓ R.1930	4-Letter Hatted (10711) 40% recovered	10/30 to 30/9/35		
B.19					
B.20	? T 1930	4-Letter		(54) 1932/34	F.O. (JEBY)
B.21					
B.22	✓ G.T.C. 1933.	5-Letter Alpha 54,000grs.	Over 3 yrs in 2/43	(55) 3/45	Used recaptured by FIRE Also used S.A., Eire, Australia, Canada
B.23		5-Letter Alpha Canadian & African (13) Slightly recovered			AUDT
B.24		5-Letter (14) Few Statistics			ANCBU

Pass Title	Book	Description	In force	Folders of Traffic	Remarks
B.25	✓ R 1935	4-Letter Hatted 16,224 grs (15) 30% recovered	Copy captured autumn '40 2/43		
B.26		5-Letter South Africa (16) Few variations		(46) 1935/39	(BEHUN)
B.27		~~5~~ 4-Letter Traffic South Africa 4 Letter bod		(47) 1938/39	(TIYS. 122A)
B.28					
B.29	? IWC				
B.30	✓ Q. 1935	4-Letter Hatted "England" (17) 40% recovered	Work began early 1942 2/43		Letts diff B.25 heavy, middle and Far East FA produced 50 grs in 2/42. Exchge with OKW 8/42
B.31	✓ R 1941	4-Letter Hatted 160000 grs	B.i.t. 1.5.42	(56) 3/45 Prodrome	Exchge with OKW from 8/42. Copied by OKM. Same Letts as B.25
Indian (? B.29)	I.W.C.	5-Letter Alpha.			

(B) Copy to D.D(CSA) 12/8. 15(Q)

Political
Turkish

TOP SECRET

TICOM/I-63

INTERROGATION REPORT ON

ORR HERMANN SCHERSCHMIDT

OF PERS. Z. S., AUSWAERTIGES AMT

The attached document is a report on the interrogation of ORR Hermann SCHERSCHMIDT of Pers. Z.S., Auswaertiges Amt, by Major W.P. Bundy, AUS and Capt. J.K. Lively, AUS at HEIDELBERG on 1st August 1945. SCHERSCHMIDT is a specialist in Turkish and Slavonic code-breaking.

TICOM
11 August 1945

No. of Pages 4

DISTRIBUTION

British
Director
D.D.3 (2)
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
A.D.(C.C.R.)(2)
Lt. Col. Leathem

U.S.
OP 20-G (2)(via Lt. Pendergrass)
G-2 (via Lt.Col.Hilles)
S.S.A. (2)(via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)

TICOM
Chairman
S.A.C. (2)
Cdr. Bacon
Cdr. McKenzie
Cdr. Tandy
Lt. Col. Johnson
Lt. Col. Lewis Powell
Lt. Cdr. Manson
Major Seaman
Lt. Eachus
Lt. Vance
Capt. Cowan
Lt. Fehl
Ticom Files (2)

Additional
Major Morgan

Interrogation Report on Oberregierungsrat

HERMANN SCHERSCHMIDT

Of Pers. Z.S., Auswaertiges Amt

At Heidelberg
1 August 1945

Interrogators:
Major W.P. Bundy, Sig. C.
Captain J.K.Lively, Sig. C.

1. Circumstances. Scherschmidt was located in the eye clinic of the Heidelberg University Hospital, recovering from a cataract operation. Although weak he was mentally clear and his answers were almost too voluble to permit notes. He was completely cooperative, and his whole attitude was exactly like that of other Pers Z.S. people. He was absolutely scientific in his approach and kept fishing for an exchange of information on the subject, appearing surprised at the ignorance of interrogators. In sum, a complete academic, of about B analytic powers.

2. Personal History. Scherschmidt is somewhat over 50 years old. Was a student in 1914, became involved in crypt in the Army, and settled down in Pers. Z. S. soon after the war to make this his life work. Except for the period March 1943 - September 1944, when personal differences caused him to transfer to straight translation work in the document translation section of the A.A., he was with Pers. Z.S. continuously until his capture at ZSCHEPPLIN on 26 April 1945.

3. Crypt Specialties. Scherschmidt was primarily engaged in the linguistic side of cryptanalysis, working on pure codes after the encipherment was removed. (The Polish diplomatic problem was an exception, as the two parts of the problem were inseparable.) Scherschmidt claims to have learned Turkish, Polish and Bulgarian in addition to a smattering of English, French, Russian, and Spanish. He was engaged entirely in Turkish work from 1934 to 1939, and in Polish from 1939 to the end of 1942. While in document translation in 1943-4 he worked on Bulgarian books (and found it very boring), and after his return he did translation and supervision of book-breaking on Turkish codes.

4. Turkish codes. Scherschmidt was not interrogated in detail on his work in Turkish. He said success was very great throughout. In the period 1934-39 the codes were unsystematic (and in Latin at least partially). In 1944-5 the code on which he worked was systematic, with a cyclic additive, and was broken easily.

5. Polish Systems. Scherschmidt worked entirely on diplomatic traffic and was not familiar with military or agent systems or with any successes achieved on them. He had dabbled in Polish throughout his Pers Z.S. career and early in 1939 he was assigned to the main diplomatic code of the Polish Foreign Office. This had been in force since 1934, and some unsuccessful research had been done in an effort to ascertain the encipherment used. The problem was given a very high priority in 1939 and Scherschmidt had first class assistance. With the aid of a captured specimen of encipherment and a captured description of the indicator system, the first message was read early

in 1940. The code was recovered gradually, and in 1941 and 1942 all messages were read, most of them currently. The code went out of use in October 1942 and was replaced by a letter code. Scherschmidt did a little work on this at first but did not come back to the problem later. He said the code was never solved, and he did not know details of the attacks made on it by KUNZE and others.

6. From 1935 to 1942 the Polish Government in Warsaw and later in London used a single unsystematic 4-digit code. The consular services used the diplomatic code of the preceding period. In the diplomatic net a separate pair of encipherment tables was provided for each outstation with one pair for broadcast messages. Scherschmidt remembered traffic to the following points from the Polish Government in LONDON: WASHINGTON (very little), CONSTANTINOPLE, MADRID, MOSCOW, ROME (the VATICAN) and BERN. Scherschmidt could not recall the contents of any of this traffic except that he did recall much talk on the MOSCOW link of negotiations between SIKORSKI and STALIN at one period. Scherschmidt remarked that the German White Paper on Poland included no traffic broken by his section; he was told that its materials were captured.

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

TICOM/I-63: Page 4 retained under S3(4) of the PRA 1958

(date) 11/2/2004

(Signed)